WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Tuesday, March 14, 2006

Hide?	Set Name	Query	Hit Count
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
☐	L51	(DVD and DRIVE and key adj exchange adj server and key adj exchange adj client).clm.	1
☐	L50	(DVD and DRIVE and authenticat$6 and key adj exchange adj server and key adj exchange adj client).clm.	0
☐	L49	386/1.ccls. and (authenticat$7 and drive$3)	3
☐	L48	386/1.ccls. and (authenticat$7 same drive$3)	1
☐	L44	725/25.ccls. and (DVD adj drive)	12
☐	L43	725/25.ccls. and (DVD adj drive same encrypt$8$7)	0
☐	L42	725/25.ccls. and (DVD adj drive same scrambl$7)	0
☐	L41	L40 and (content same DVD same drive)	2
☐	L40	(713/171 |713/380).ccls.	531
☐	L39	DVD adj changer$2 and key	21
☐	L38	DVD adj changer$2 same key	4
☐	L37	DVD adj changer$2 and key adj exchange	1
☐	L36	changer and key adj exchange	11
☐	L35	DVD adj changer and key adj exchange	1
☐	L34	jukebox and key adj exchange	20
☐	L33	jukebox same key adj exchange	0
☐	L32	DVD adj jukebox and (encrypt$7 same key)	3
☐	L31	DVD adj jukebox same encrypt$7	3
☐	L30	L27 and home adj network	7
☐	L29	L27 same home adj network	0
☐	L28	L27 same homenetwork	0
☐	L27	DVD adj drive same encrypt$7	104
☐	L26	DVD adj changer and encrypt$7	8
☐	L25	DVD adj changer same encrypt$7	3
☐	L24	L21 same key same encrypt$7	1
☐	L23	L21 and copy adj protection	0
☐	L22	L21 same copy adj protection	0
☐	L21	jukebox near3 server	140
☐	L20	jukebox near3 server and hoem adj network	0

☐	L19	jukebox near3 server same hoem adj network	0
☐	L18	jukebox adj server same hoem adj network	0
☐	L17	jukebos adj server same hoem adj network	0
☐	L16	6,055,314.pn.	2
☐	L15	home adj network same (DVD same key)	15
☐	L14	L12 same key	8
☐	L13	L12 near4 key	1
☐	L12	jukebox near4 server	179
☐	L11	server near4 DVD adj changer and key	1
☐	L10	server near4 DVD adj changer and key	1
☐	L9	server near4 DVD adj changer	4
☐	L8	L7 and encrypt$7	4
☐	L7	(DVD near2 changer$3) and (key)	47
☐	L6	(DVD near2 changer$3) and (encryption same key)	1
☐	L5	(DVD near2 changer same key)	8
☐	L4	DVD near2 changer near3 key	2
☐	L3	pass$6 near4 key near3 DVD	7
☐	L2	DVD adj drive near10 client near10 server	16
☐	L1	6,546,193.pn.	4

END OF SEARCH HISTORY

WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Tuesday, March 14, 2006

Hide?	Set Name	Query	Hit Count
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
☐	L59	L56 and (content$6 same DVD same Drive)	2
☐	L58	L56 and (drive same authenticat$7)	14
☐	L57	L56 and (drive near2 authenticat$7)	0
☐	L56	713/171.ccls.	531
☐	L55	380/201.ccls. and (DVD adj drive and authenticat$8 and key adj exchange)	5
☐	L54	380/201.ccls. and (DVD adj drive and authenticat$8 and key adj exchange adj server)	0
☐	L53	380/201.ccls. and (DVD adj drive same authenticat$8)	10
☐	L52	380/201.ccls. and (DVD adj drive same authenticate same network)	0
☐	L51	(DVD and DRIVE and key adj exchange adj server and key adj exchange adj client).clm.	1
☐	L50	(DVD and DRIVE and authenticat$6 and key adj exchange adj server and key adj exchange adj client).clm.	0
☐	L49	386/1.ccls. and (authenticat$7 and drive$3)	3
☐	L48	386/1.ccls. and (authenticat$7 same drive$3)	1
☐	L44	725/25.ccls. and (DVD adj drive)	12
☐	L43	725/25.ccls. and (DVD adj drive same encrypt$8$7)	0
☐	L42	725/25.ccls. and (DVD adj drive same scrambl$7)	0
☐	L39	DVD adj changer$2 and key	21
☐	L38	DVD adj changer$2 same key	4
☐	L37	DVD adj changer$2 and key adj exchange	1
☐	L36	changer and key adj exchange	11
☐	L35	DVD adj changer and key adj exchange	1
☐	L34	jukebox and key adj exchange	20
☐	L33	jukebox same key adj exchange	0
☐	L32	DVD adj jukebox and (encrypt$7 same key)	3
☐	L31	DVD adj jukebox same encrypt$7	3
☐	L30	L27 and home adj network	7
☐	L29	L27 same home adj network	0
☐	L28	L27 same homenetwork	0
☐	L27	DVD adj drive same encrypt$7	104
☐	L26	DVD adj changer and encrypt$7	8

☐	L25	DVD adj changer same encrypt$7	3
☐	L24	L21 same key same encrypt$7	1
☐	L23	L21 and copy adj protection	0
☐	L22	L21 same copy adj protection	0
☐	L21	jukebox near3 server	140
☐	L20	jukebox near3 server and hoem adj network	0
☐	L19	jukebox near3 server same hoem adj network	0
☐	L18	jukebox adj server same hoem adj network	0
☐	L17	jukebos adj server same hoem adj network	0
☐	L16	6,055,314.pn.	2
☐	L15	home adj network same (DVD same key)	15
☐	L14	L12 same key	8
☐	L13	L12 near4 key	1
☐	L12	jukebox near4 server	179
☐	L11	server near4 DVD adj changer and key	1
☐	L10	server near4 DVD adj changer and key	1
☐	L9	server near4 DVD adj changer	4
☐	L8	L7 and encrypt$7	4
☐	L7	(DVD near2 changer$3) and (key)	47
☐	L6	(DVD near2 changer$3) and (encryption same key)	1
☐	L5	(DVD near2 changer same key)	8
☐	L4	DVD near2 changer near3 key	2
☐	L3	pass$6 near4 key near3 DVD	7
☐	L2	DVD adj drive near10 client near10 server	16
☐	L1	6,546,193.pn.	4

END OF SEARCH HISTORY

STIC SEARCH REPORT

Set	Items	Description
S1	1171561	STORAGE()(MEDIA? ? OR MEDIUM? ?) OR DVD OR DISK? OR DISC? ? OR CD OR CD()ROM OR TAPE? ? OR (DAT OR DIGITAL()ANALOG OR CASSETTE)()TAPE? ?
S2	6826	((COMPUTER? OR CLIENT??? OR HANDHELD? OR USER? ? OR PDA OR PALM()PILOT? OR HANDSET? ? OR DESKTOP?? OR LAPTOP??)(3N)(DEVICE? OR INSTRUMENT? OR MECHANISM? OR UNIT? OR APPARAT? OR HARDWARE? OR (HARD OR CD OR DVD)()DRIVE?))(7N)S1
S3	7851013	RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?
S4	125648	CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTHORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S5	262762	KEY???
S6	3404	STREAM???()(MEDIA()CONTENT? ? OR VIDEO??? OR AUDIO???) OR (DELIVER??? OR SEND??? OR DOWNLOAD??? OR UPLOAD???)(3N)(REAL()TIME OR REALTIME OR LIVE OR IMMEDIAT? OR INSTANT? OR UP(3W)(MINUTE? OR SECOND? OR MOMENT?))
S7	13306	(NETWORK? OR NET? ? OR INTERNET? OR INTRANET? OR ONLINE OR WAN? ? OR LAN? ? OR ETHERNET? OR EXTRANET? OR WWW OR WORLD()WIDE()WEB OR WORLDWIDEWEB OR SUBNET? OR SERVER? ? OR WEB()SERVER? ?)(10N)S1
S8	186529	DECRYPT? OR DECIPHER? OR DECOD? OR UNSCRAMBL? OR DESCRAMBL?
S9	1606536	IC=(G06F? OR H04L?)
S10	1838891	MC=(T01? OR W02? OR W04?)
S12	300	S1 AND S3 AND S4(5N)S5
S13	10	S12 AND S2 AND S3 AND S4(5N)S5
S14	10	S12 AND S2 AND S3 AND S4(7N)S5
S15	7885	S4(10N)S5
S16	16	S15 AND S4(5N)S5 AND S4 AND S2
S17	6336	STREAM???()(MEDIA()CONTENT? ? OR VIDEO??? OR AUDIO???) OR (DELIVER??? OR SEND??? OR DOWNLOAD??? OR UPLOAD???)(3N)(REAL()TIME OR REALTIME OR LIVE OR IMMEDIAT? OR INSTANT? OR STREAM??? OR UP(3W)(MINUTE? OR SECOND? OR MOMENT?))
S18	1007	(NETWORK? OR NET? ? OR INTERNET? OR INTRANET? OR ONLINE OR WAN? ? OR LAN? ? OR ETHERNET? OR EXTRANET? OR WWW OR WORLD()WIDE()WEB OR WORLDWIDEWEB OR SUBNET? OR SERVER? ? OR WEB()SERVER? ?)(10N)S17
S19	6	S16 NOT S14
S20	0	S18 AND S1 AND S3 AND S4(5N)S5
S21	0	S18 AND S2 AND S3 AND S4(5N)S5
S22	950	S18 AND S9:S10
S23	6	S22 AND S3 AND S4 AND S5
S24	6	S23 NOT S16
S25	0	S22 AND S4(5N)S5 AND S4 AND S2
S26	8	S8 AND S4(7N)S5 AND S4 AND S2
S27	0	S26 NOT (S16 OR S24)
S28	2	S22 AND S2
S29	11	S2 AND S3 AND S4(7N)S5
S30	13	S28:S29
S31	3	S30 NOT (S16 OR S24 OR S26)
S32	0	S17 AND S2 AND S3 AND S4 AND S5 AND S1
S33	2	S17 AND S1 AND S3 AND S4(10N)S5
S34	2	S17 AND S1 AND S3 AND S4(10N)S5
S35	2	S33:S34
S36	0	S35 NOT S23:S33
S37	509	AU=(CHAN S? OR CHAN, S?)
S38	10	AU=(MAYMUDES D? OR MAYMUDES, D?)
S39	0	SHANNON(2N)CHAN OR (DAVE OR DAVID)(2N)MAYMUDES
S40	1	S37 AND S38
S41	143	S37:S38 AND S9:S10

```
S42          15   S41 AND S1
S43           0   S41 AND S18
S44           1   S41 AND S6
S45           3   S41 AND S2
S46           0   S41 AND S4(10N)S5
S47           1   S44:S45 NOT S42
S48           1   S47 NOT S40
S49           1   S41 AND S7
S50           0   S49 NOT S42:S48
S51         231   S12 AND S4(3N)S5
S52           5   S51 AND S4 AND S2
S53          48   S51 AND S3 AND S4 AND (S7 OR S18)
S54          52   S52:S53
S55          44   S54 NOT PR=2002:2006
S56          51   S19 OR S23:S36 OR S38:S40 OR S42:S50
S57          39   S55 NOT S56
S58          39   IDPAT (sorted in duplicate/non-duplicate order)
File 347:JAPIO Nov 1976-2005/Nov(Updated 060302)
         (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200616
         (c) 2006  Thomson Derwent
```

14/3,K/8 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014735538 **Image available**
WPI Acc No: 2002-556242/200259
XRPX Acc No: N02-440199
Distributed file system for storage devices network, has key manager maintaining encryption-decryption keys used by clients to encrypt-decrypt data in storage devices and lock manager for encrypted data transfer
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: BURNS R C; CHRON E G; LONG D; REED B C
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6405315	B1	20020611	US 97927772	A	19970911	200259	B

Priority Applications (No Type Date): US 97927772 A 19970911
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6405315	B1		20	G06F-011/30	

... by clients to encrypt-decrypt data in storage devices and lock manager for encrypted data transfer
Abstract (Basic):
... A key manager maintains various encryption and decryption **keys** which are used by respective **authorized** client to remotely encrypt and decrypt data objects accessed from a storage device. A lock manager maintains data consistency while **transferring** encrypted data files and metadata describing a directory structure in secured manner from one storage...
... For network of storage devices such as direct access **disk** drives (DASD), optical storage **disks** , **tape** drives, **computers** and **instruments** having storage **units** or combination of **computers** and **instru**ments to implement virtual file system (VFS) used by UNIX...

...performed only by a client, overhead to a storage device is reduced. Since data is **transferred** directly between the storage devices, overhead to a client is minimized...
...Title Terms: **TRANSFER**

14/3,K/9 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013281610 **Image available**
WPI Acc No: 2000-453545/200040
XRPX Acc No: N00-337824
Data storage apparatus for electronic documents e.g. contracts,domicile certificates on data networks using key management function unique to data storage when transmitting or receiving
Patent Assignee: FUJITSU LTD (FUIT)
Inventor: IWASE S; KAMADA J; KURODA Y; NODA B; ONO E
Number of Countries: 027 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1011222	A2	20000621	EP 99304647	A	19990615	200040	B
JP 2000181803	A	20000630	JP 98360345	A	19981218	200043	
US 6915434	B1	20050705	US 99327477	A	19990608	200544	

Priority Applications (No Type Date): JP 98360345 A 19981218
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1011222	A2	E	38	H04L-009/08	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
JP 2000181803	A		23	G06F-012/14	
US 6915434	B1			H04L-009/32	

Data storage apparatus for electronic documents e.g. contracts,domicile certificates on data networks using key management function unique to data storage when transmitting or receiving

Abstract (Basic):
... apparatus (10) is managed by key management unit (12).The encryption unit (13) generates a **key** ,encrypts and **verifies** the electronic data. The **key** storage unit (14,15,16) stores key unique to data as individual, group or public. And a communication unit (18) is used for **transmitting** and **receiving** electronic data on a network.
... INDEPENDENT CLAIM is also included for a method of managing electronic data in a storage **apparatus** , a computer program product stored on a computer readable **storage medium** .
...

...For electronic documents e.g. contracts,domicile certificates **transmitted** or **received** on a data network...

...The security of data is guaranteed by **transmitting** to and **receiving** from another storage device after re-encrypting using a common **key** shared with **receiving** apparatus when **verification** result is correct
...Title Terms: **TRANSMIT** ;

14/3,K/10 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009359632 **Image available**
WPI Acc No: 1993-053111/199231
XRPX Acc No: N93-040649
Computer **security** device **for permitting limited access to** storage media **- has logic circuit located in series between** disk **drive and** disk **controller which is key operable to allow selective disable or enable**
Patent Assignee: KIVELL S N (KIVE-I)
Inventor: KIVELL S N
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
ZA 9104447	A	19920624	ZA 914447	A	19910611	199231	B

Priority Applications (No Type Date): ZA 902420 A 19900329
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
ZA 9104447	A		7	G06C-000/00	

Computer **security** device **for permitting limited access to** storage media - ...
...**has logic circuit located in series between** disk **drive and** disk **controller which is key operable to allow selective disable or enable**

...Abstract (Basic): The device includes the logic circuit (12) operable by a **key** (14), card or code of an **authorised** person and is located in series between the **disc** , drive and the **disc** controller for the data and control signals to the **disc** drive to be controlled...

...The **key** is adopted to enable an **authorised** person to selectively disable or enable the **disc** read/write of the computer circuitry. If the floppy drive is write protected an unauthorised...

...held in the hard drive and when write protected it will not be possible to **transfer** a virus onto the hard drive of the **disc** .

...Title Terms: **DISC** ;

19/3,K/6 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014612937 **Image available**
WPI Acc No: 2002-433641/200246
XRPX Acc No: N02-341207
Public key management method for communication system, involves verifying whether public key certificate related to security operation is authentic, based on which notification is performed to client application
Patent Assignee: ENTRUST TECHNOLOGIES LTD (ENTR-N)
Inventor: VAN OORSCHOT P C
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6370249	B1	20020409	US 97901054	A	19970725	200246	B

Priority Applications (No Type Date): US 97901054 A 19970725
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6370249	B1		15	H04L-009/00	

Public key management method for communication system, involves verifying whether public key certificate related to security operation is authentic, based on which notification is performed to client application

Abstract (Basic):
... A client cryptographic engine is evoked by a client application to determine whether a public **key certificate** associated with the security related operation, is authentic. The cryptographic engine indicates that the security...
... 2) Trust **certification** authority...

...4) Digital **storage medium** comprising program for causing processing **unit** to function as **client** cryptographic engine...

...The public key management method allows online real time updating of trusted public **keys** of **certification** authorities by enabling communication between client end cryptographic engines. Secure communication system is more flexible...

... **Certification** authorities (34,46,58
...Title Terms: **VERIFICATION** ;

31/3,K/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016516974 **Image available**
WPI Acc No: 2004-675357/200466
Related WPI Acc No: 2004-354636
XRPX Acc No: N04-535163
Data server **information services integrating computer program product, has instructions to** deliver **information from** real - time **information source with higher priority than sub-portion of non-real-time** information
Patent Assignee: DIGITAL INTEGRATOR INC (DIGI-N)
Inventor: GISSEL P V; HAHN C P
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20040177156	A1	20040909	US 2000702989	A	20001101	200466 B
			US 2004801572	A	20040317	

Priority Applications (No Type Date): US 2000702989 A 20001101; US 2004801572 A 20040317
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040177156	A1		12	G06F-015/16	Cont of application US 2000702989 Cont of patent US 6725446

Data server **information services integrating computer program product, has instructions to** deliver **information from** real - time **information source with higher priority than sub-portion of non-real-time information**

Abstract (Basic):
... The product has a **computer** program code **mechanism** embedded in a **computer storage medium** . The **mechanism** has instructions to receive information from real-time information sources, and to receive a sub...
International Patent Class (Main): **G06F-015/16**
International Patent Class (Additional): **G06F-015/173**
Manual Codes (EPI/S-X): **T01-N01A2** ...

... **T01-N02B1A** ...

... **T01-S01B** ...

... **T01-S03**

Your Application

40/3,K/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015187209 **Image available**
WPI Acc No: 2003-247742/200324
XRPX Acc No: N03-196949

Security key exchange system for streaming protected media content on DVD, communicates one or more keys from DVD of server device to key exchange client, to allow decoder to decrypt content received from DVD

Patent Assignee: CHAN S J (CHAN-I); MAYMUDES D M (MAYM-I)
Inventor: **CHAN S J** ; **MAY**MUDES D M
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030009668	A1	20030109	US 2001882810	A	20010614	200324	B

Priority Applications (No Type Date): US 2001882810 A 20010614
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030009668	A1		17	H04L-009/00	

Inventor: **CHAN S J** ...

42/3,K/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015378841 **Image available**
WPI Acc No: 2003-439779/200341
Related WPI Acc No: 2003-074611; 2003-327733
XRPX Acc No: N03-350968

Computer-readable medium stores data structure with packets having reference count field which is examined to detect whether reference field of packet includes reference to location of specific variable-size data object

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: **CHAN S** ; SHUM H
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20030055833	A1	20030320	US 99471678	A	19991223	200341 B
			US 99471932	A	19991223	
			US 2002285138	A	20021030	

Priority Applications (No Type Date): US 99471678 A 19991223; US 99471932 A 19991223; US 2002285138 A 20021030
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030055833	A1		45	G06F-007/00	Cont of application US 99471678 Div ex application US 99471932 Cont of patent US 6476805 Div ex patent US 6502097

Inventor: **CHAN S** ...

Abstract (Basic):
... 4) **storage medium** with data structure filling program; and
...

...5) **storage medium** with variable-size data object accessing program
...
International Patent Class (Main): **G06F-007/00**
Manual Codes (EPI/S-X): **T01-N01D1** ...

... **T01-N02A** ...

... **T01-S03** ...

... **W02-K03** ...

... **W04-F01F** ...

... **W04-G01F**

42/3,K/14 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009958915 **Image available**
WPI Acc No: 1994-226628/199428
XRPX Acc No: N94-178645
Video data compression method for recording movies on CD ROM - setting characteristic values of pixel groups forming video frame and falling within specified variance limits to same value
Patent Assignee: MICROSOFT CORP (MICR-N)
Inventor: LANEY S T; LEDOUX E; **MAYMUDES D M** ; MILLER D J
Number of Countries: 020 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 606629	A2	19940720	EP 93120627	A	19931221	199428	B
CA 2112051	A	19940623	CA 2112051	A	19931221	199433	
JP 7075090	A	19950317	JP 93354832	A	19931222	199520	
US 5467134	A	19951114	US 92995504	A	19921222	199551	
EP 606629	A3	19960221	EP 93120627	A	19931221	199622	
JP 3306207	B2	20020724	JP 93354832	A	19931222	200255	

Priority Applications (No Type Date): US 92995504 A 19921222
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 606629	A2	E	46	H04N-005/92	
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE					
CA 2112051	A			H04N-007/12	
JP 7075090	A		38	H04N-007/24	
US 5467134	A		37	H04N-007/26	
EP 606629	A3			H04N-005/92	
JP 3306207	B2		36	H04N-007/24	Previous Publ. patent JP 7075090

Video data compression method for recording movies on CD ROM -
...Inventor: **MAYMUDES D M**
...Title Terms: **CD** ;
Manual Codes (EPI/S-X): **T01-D02** ...

... **T01-J10A1** ...

... **T01-J10B** ...

... **W04-C10A3** ...

... **W04-F01F1** ...
... **W04-K05**

58/3,K/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017293623 **Image available**
WPI Acc No: 2005-617252/200563
Related WPI Acc No: 2000-611744; 2000-647267; 2000-647268; 2001-090815; 2001-191170; 2001-210824; 2001-210825; 2001-496746; 2001-522158; 2001-522159; 2001-596328; 2001-596397; 2002-279866; 2002-392575; 2003-522656; 2005-701313
XRPX Acc No: N05-506645

Interdependent validation **method for protecting digital data content in digital rights management system, involves using private** key **that** validates **digital** signatures of digital content package and license

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: BLINN A N; JONES T C
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20050192907	A1	20050901	US 99126614	P	19990327	200563 B
			US 99290363	A	19990412	
			US 2000482928	A	20000113	
			US 2005117590	A	20050428	

Priority Applications (No Type Date): US 99126614 P 19990327; US 99290363 A 19990412; US 2000482928 A 20000113; US 2005117590 A 20050428
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050192907	A1		34	G06F-017/60	Provisional application US 99126614
					Cont of application US 99290363
					Div ex application US 2000482928

Interdependent validation **method for protecting digital data content in digital rights management system, involves using private** key **that** validates **digital signatures of digital content package and license**

Abstract (Basic):

... private key is derived from a source node of a client device, in order to **validate** the digital signature **obtained** from digital content package. A private key is derived from the previous private **key** in order to **validate** another digital signature **obtained** from the license.

... For enforcing independent **validation** of digital contents in digital rights management system using tangible devices like magnetic **tape** , floppy **disk** , and optical **disk** and intangible media like electronic bulletin board, electronic **network** and **internet** .

...

...Provides **validation** of digital content package having a portion of digital content in encrypted form with corresponding

58/3,K/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016721661 **Image available**
WPI Acc No: 2005-045936/200505
XRPX Acc No: N05-040053
Communication method of audio/video data between electronic devices e.g. digital television, involves accessing information related to communication state by electronic source device for properly processing communication commands
Patent Assignee: SONY CORP (SONY); SONY ELECTRONICS INC (SONY)
Inventor: SUN J S
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6826699	B1	20041130	US 2000692672	A	20001019	200505	B

Priority Applications (No Type Date): US 2000692672 A 20001019
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6826699	B1		12	G06F-011/30	

Abstract (Basic):
... packets is simultaneously performed between single electronic source device and two electronic sink devices using **authentication** and **key** exchange protocols. A table is created for recording information related to the communication state. The...
... device such as personal computer, digital television, digital video cassette recorder, digital set top box, **DVD** drive, digital audio/video **receiver** and digital camera, through **network** .
...

...are properly processed by the source device, the multiple audio/video data packets are simultaneously **transmitted** from single source device to multiple sink devices using various **authentication** and **key** exchange protocols, thereby maximizing bandwidth of communication network...

...the flowchart illustrating communication method of digital electronic source device and multiple sink devices using **authentication** and **key** exchange protocols

58/3,K/19 (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015215438 **Image available**
WPI Acc No: 2003-275975/200327
XRPX Acc No: N03-219213
On-line encrypted media files auditing method involves authenticating **user by measuring** key **stroke dynamics of information entry made by user and according to selected encrypted media file of auditing device**
Patent Assignee: MUSICRYPT INC (MUSI-N); HEAVEN J (HEAV-I); HUNT C (HUNT-I); STAPLES D (STAP-I); STEINMAN S (STEI-I)
Inventor: HEAVEN J; HUNT C; STAPLES D; STEINMAN S
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020188854	A1	20021212	US 2001875987	A	20010608	200327	B
CA 2349797	A1	20021207	CA 2349797	A	20010607	200327	N
US 7003670	B2	20060221	US 2001875987	A	20010608	200615	

Priority Applications (No Type Date): US 2001875987 A 20010608; CA 2349797 A 20010607
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020188854	A1		14	H04L-009/32	
CA 2349797	A1	E			
US 7003670	B2			H04L-009/00	

On-line encrypted media files auditing method involves authenticating **user by measuring** key **stroke dynamics of information entry made by user and according to selected encrypted media file...**

Abstract (Basic):
... A biometric profile of an **authenticated** user created by measuring keystroke dynamics of information entry including password, user name, address made...

...is compared with the prestored measured biometric profile. A selected encrypted media file from a **storage medium** is streamed over a **network** and decrypted to an auditing device, if the individual is **verified** as the **authenticated** user.
... 3) computer program product comprises **storage medium** for storing on-line encrypted media files auditing program...

...For allowing **authorized** user to audit encrypted media files through network...

...As the encrypted media files are **downloaded** to the **authorized** user only after comparing the measured key stroke dynamics with the prestored measured value, a secure and user-friendly system for accessing and **downloading** on-line media is provided...

58/3,K/27 (Item 27 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014036998 **Image available**
WPI Acc No: 2001-521211/200157
XRPX Acc No: N01-386131
System for obtaining **digital information via a communication network such as the Internet using a server with a list of computer games and a server including a storage device**
Patent Assignee: MEDIA STATION INC (MEDI-N)
Inventor: FLURRY H S; STINSON J L
Number of Countries: 094 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200101240	A2	20010104	WO 2000US17359	A	20000623	200157 B
AU 200057629	A	20010131	AU 200057629	A	20000623	200157

Priority Applications (No Type Date): US 99347584 A 19990630
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200101240	A2	E	22	G06F-009/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

AU 200057629	A		G06F-009/00	Based on patent WO 200101240	

System for obtaining **digital information via a communication network such as the Internet using a server with a...**

Abstract (Basic):
... present a client machine (120) with a selection of titles via the Internet (150). A **server** table (116) provides a list of various scenes on which **CD - ROM** images are stored and a user can play a game title using web pages (117) after **obtaining authorization** and a **CD key** file (119). A web browser (121) provides a user interface and **obtains** the **CD** key file (122) for selecting an image of a computer game at the server and...
... **Obtaining** digital information from **CD** formatted data via a communication **network** .
...

... **CD** key files (119,122
...Title Terms: **OBTAIN** ;

58/3,K/30 (Item 30 from file: 350)

012745413 **Image available**
WPI Acc No: 1999-551530/199946
XRPX Acc No: N99-408080

Network communication security method using ultra long identification key codes and-or ultra large databases of identification key codes, for e.g. Internet and Intranet

Patent Assignee: NEWTON F (NEWT-I); WILLIAMS G (WILL-I)
Inventor: NEWTON F; WILLIAMS G
Number of Countries: 073 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9946691	A1	19990916	WO 98US10355	A	19980522	199946	B
AU 9877971	A	19990927	AU 9877971	A	19980522	200006	
JP 2002507025	W	20020305	WO 98US10355	A	19980522	200220	
			JP 2000536009	A	19980522		

Priority Applications (No Type Date): US 9837297 A 19980309
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9946691	A1	E	72	G06F-015/20	
	Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN				
	Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL PT SD SE SZ UG ZW				
AU 9877971	A			G06F-015/20	Based on patent WO 9946691
JP 2002507025	W		55	G06F-015/00	Based on patent WO 9946691

Abstract (Basic):

... of individualized and class specific access key code and optional individual encryption key generated by **key** generation algorithms. Each **authorized** user is provided with **storage media** containing the user's individual or class specific access key code.

... The host computer is provided with a program for comparing **transmitted** individual and class specific access **key** codes and stored **authorized** access **key**' codes, and for permitting correct matches to have access to the server transaction program. The...

...permitting connection to the host computer through a communication network or telephone network, and for 1transmitting individualized and class specific access key codes through the remote computer terminal to the host...

...access to host computer. Erases transactions of the connection if proper exit code is not **received** , thus aborting a hijacked connection. Thwarts trespassing attacks on the security system, and allows trespassers...

...to be identified. Enables passwords of hundreds of characters to be readily employed by using **CD - ROM disk** key...

...The figure shows a schematic diagram illustrating various steps required to practice the **network** communications security system, and the hardware and software of one **CD - ROM** .

58/3,K/31 (Item 31 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011499047 **Image available**
WPI Acc No: 1997-476960/199744
XRPX Acc No: N97-397744
Portable data recording medium authentication **method for commercial transaction - by** obtaining **digital signature that includes open** key **and secret** key **used in** authentication **operation of public** key **cryptic system, from portable data recording medium**
Patent Assignee: DAINIPPON PRINTING CO LTD (NIPQ)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 9223210	A	19970826	JP 9653646	A	19960219	199744	B

Priority Applications (No Type Date): JP 9653646 A 19960219
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9223210	A		7	G06K-017/00	

Portable data recording medium authentication **method for commercial transaction...**
...by obtaining **digital signature that includes open** key **and secret** key **used in** authentication **operation of public** key **cryptic system, from portable data recording medium**

...Abstract (Basic): The method entails **obtaining** a digital signature from a portable data recording medium (10) such as an integrated circuit...

...includes an open key (2) and a secret key (1) which are used in an **authentication** operation of a public **key** cryptic system...

...ADVANTAGE - Safely manages **key** used in **authenticating** digital signature since unauthorised usage and alterations are prevented. Keeps key in portable data recording medium thereby eliminating need to store key in magnetic **disk** of **network** terminal...
...Title Terms: **OBTAIN** ;

58/3,K/38 (Item 38 from file: 347)
DIALOG(R)File 347:JAPIO

06890370 **Image available**
INFORMATION PROCESSOR, **NETWORK** SYSTEM, METHOD FOR MANAGING CUSTOMER AND **STORAGE MEDIUM**

PUB. NO.: 2001-117879 [JP 2001117879 A]
PUBLISHED: April 27, 2001 (20010427)
INVENTOR(s): FUJIKAWA SHINJI
FUKUNAGA SHINJI
INOSE ATSUSHI
APPLICANT(s): CANON INC
APPL. NO.: 11-294450 [JP 99294450]
FILED: October 15, 1999 (19991015)

INFORMATION PROCESSOR, **NETWORK** SYSTEM, METHOD FOR MANAGING CUSTOMER AND **STORAGE MEDIUM**

ABSTRACT
... adds specified information (information of privilege, etc.), concerning the service of the store to an **authenticating key** for permitting the utilization of the service to a user 103(X) and **transmits** it to a server 101. The server 101 permits the utilization of the service of the store based on the **authenticating key** to the user when the **authenticating key** issued by the store terminal equipment 102(X) is inputted from the user 103(X...

58/3,K/39 (Item 39 from file: 347)
DIALOG(R)File 347:JAPIO

06099709 **Image available**
METHOD AND SYSTEM FOR **AUTHENTICATING** USER

PUB. NO.: 11-041230 [JP 11041230 A]
PUBLISHED: February 12, 1999 (19990212)
INVENTOR(s): HASHIGUCHI MASAHIRO
APPLICANT(s): YOKOGAWA DIGITAL COMPUTER KK
APPL. NO.: 09-196843 [JP 97196843]
FILED: July 23, 1997 (19970723)

METHOD AND SYSTEM FOR **AUTHENTICATING** USER

ABSTRACT

PROBLEM TO BE SOLVED: To provide a method and a system for **authenticating** user with which sure security can be kept while using an inexpensive **storage medium** (such as a floppy **disk**), in place of a cript card.

SOLUTION: In the system composed of a controller and...

... controller, on the side of the operating part, a means is provided for reading the **storage medium** , in which a specified parameter is stored, and generating a user **certification** code from this parameter and a parameter applied from the controller while using a specified function. On the other hand, on the side of the controller, an **authentication** manager 11 is provided for generating a specified code based on the parameter sent from the **storage medium** while using the specified function, and an **authentication Web server** 12 is provided for **downloading** an applet for **authentication** to an accessing browser, **certifying** a CRL with **key** sent from the operating part, **acquiring** a relevant page from a linked Web server 1 and displaying it on a display...

```
Set     Items   Description
S1     517946   STORAGE()(MEDIA? ? OR MEDIUM? ?) OR DVD OR DISK? OR DISC? ?
              OR CD OR CD()ROM OR TAPE? ? OR (DAT OR DIGITAL()ANALOG OR CA-
             SSETTE)()TAPE? ?
S2      10468   ((COMPUTER? OR CLIENT??? OR HANDHELD? OR USER? ? OR PDA OR
             PALM()PILOT? OR HANDSET? ? OR DESKTOP?? OR LAPTOP??)(3N)(DEVI-
             CE? OR INSTRUMENT? OR MECHANISM? OR MACHINE? ? OR UNIT? OR AP-
             PARAT? OR HARDWARE? OR (HARD OR CD OR DVD)()DRIVE?))(5N)S1
S3        121   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
             HORIZ? OR AUTHORIS? OR APPROV? OR VERIF?)(10N)S2
S4     236969   KEY???
S5      12331   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
             HORIZ? OR AUTHORIS? OR APPROV? OR VERIF?)(5N)S4
S6       4616   (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
             DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
             OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?)(-
             7N)S5

S7         66   (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
             DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
             OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?)(-
             5N)(S1(7N)S5)
S8    1957059   RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR -
             DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
             OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?
S9     277117   CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
             ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S10    123995   DECRYPT? OR DECIPHER? OR DECOD? OR UNSCRAMBL? OR DESCRAMBL?
S11     22577   STREAM???()(MEDIA()CONTENT? ? OR VIDEO??? OR AUDIO???) OR -
             (DELIVER??? OR SEND??? OR DOWNLOAD??? OR UPLOAD???)(3N)(REAL(-
             )TIME OR REALTIME OR LIVE OR IMMEDIAT? OR INSTANT? OR STREAM?-
             ?? OR UP(3W)(MINUTE? OR SECOND? OR MOMENT?))
S12      4469   (NETWORK? OR NET? ? OR INTERNET? OR INTRANET? OR ONLINE OR
             WAN? ? OR LAN? ? OR ETHERNET? OR EXTRANET? OR WWW OR WORLD()W-
             IDE()WEB OR WORLDWIDEWEB OR SUBNET? OR SERVER? ? OR WEB()SERV-
             ER? ?)(10N)S11
S13    228847   IC=(G06F? OR H04L?)
S14         1   S12 AND (S5(5N)S1)(10N)S3
S15         1   S12 AND S2(10N)S6
S16         9   S12 AND S3
S17       157   S12 AND S6
S18         1   S17 AND S2(10N)S6
S19         9   S14:S16 OR S18
S20        11   S17 AND S5(10N)S1
S21         8   S20 NOT S19
S22        85   S17 NOT AD=2002:2006
S23        65   S3 NOT AD=2002:2006
S24     21621   (EXCHANG? OR RECIPROC??? OR REVERS? OR SWAP OR SWAPS OR SW-
             APPING OR TRADE? ? OR TRADING OR SWITCH? OR TRANSACT?)(7N)(S4-
             :S5)
S25      1040   (INTERMEDIAR??? OR GO()BETWEEN? ? OR MIDDLEMAN OR PROXY OR
             BROKER?  OR NEGOTIATOR? OR VENDOR?)(5N)S4:S5
S26      1253   (SURROGAT? OR EMISSAR? OR INTERCESSOR? OR MEDIATOR? OR INT-
             ERAGENT? OR FINANCIER? OR PROPRIET?)(5N)S4:S5
S27      4779   (AGENT? ? OR REPRESENTATIVE? OR ARBITRATOR? OR PROMOTER? OR
              MEDIAR? OR EXECUTOR OR SUBSTITUT?)(5N)S4:S5
S28      6872   S25:S27
S29         0   (S2(10N)S24)(10N)S28
S30         1   S28(10N)S3
S31         1   S28(50N)S3
S32         1   (S1 OR S11:S12) AND S28(10N)S2
```

23/3,K/57 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00529396
DATA DISC MODULATION FOR MINIMIZING PIRATING
MODULATION D'UN DISQUE DE DONNEES PERMETTANT DE REDUIRE AU MAXIMUM LE PIRATAGE
Patent Applicant/Assignee:
RECORDING INDUSTRY ASSOCIATION OF AMERICA,
STEBBINGS David W,
Inventor(s):
STEBBINGS David W,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9960748 A1 19991125
Application: WO 99US11184 19990520 (PCT/WO US9911184)
Priority Application: US 9886132 19980520
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IN IS JP KE KG KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 19215

Fulltext Availability:
Detailed Description

Detailed Description
... within encrypted information that is burned into the disc. Authentication keys are buried using various **authentication** processes, which **verify** that the platform **device** - whether a **computer** , **CD** player, **DVD** player, or the like - is a licensed device and, consequently, obeys certain copyright rules. Eventually...

23/3,K/56 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00561872 **Image available**
MECHANISM FOR MULTIPLE PARTY NOTARIZATION OF ELECTRONIC TRANSACTIONS
MECANISME DE NOTARISATION DE PLUSIEURS CORRESPONDANTS PARTICIPANT A DES TRANSACTIONS ELECTRONIQUES
Patent Applicant/Assignee:
RECEIPT COM INC,
Inventor(s):
JEVANS David,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200025245 A1 20000504 (WO 0025245)
Application: WO 99US24570 19991020 (PCT/WO US9924570)
Priority Application: US 98105778 19981027; US 98223691 19981230
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 13228

Fulltext Availability:
Claims

Claim
... transaction document; and
(c) provide said verified electronic transaction document and an indication of said **verification** to said issuer party participant.

40 A computer readable **storage medium** for use with **computer apparatus** ,
said medium carrying **computer** instructions which, when executed by said computer
apparatus:
(a) receive an electronic transaction document, said...

. . .

. . .

23/3,K/54 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00743135
INTERNET, INTRANET AND OTHER NETWORK COMMUNICATION SECURITY SYSTEMS UTILIZING ENTRANCE AND EXIT KEYS
INTERNET, INTRANET ET AUTRES SYSTEMES DE SECURITE POUR COMMUNICATION EN RESEAU UTILISANT DES CLES D'ENTREE ET DE SORTIE
Patent Applicant/Assignee:
NEWTON Farrell, 8 Brighton 10th Path, Brooklyn, NY 11235, US, US (Residence), US (Nationality)
Patent Applicant/Inventor:
WILLIAMS Gareth, 8 Brighton 10th Path, Brooklyn, NY 11235, US, US (Residence), US (Nationality)
MOORE Charles E II, 35-11 85th Street, Jackson Hts, NY 11372, US, US (Residence), US (Nationality)
NICHOLS Christopher M, 80 Varick Street, New York, NY 10013, US, US (Residence), US (Nationality)
Legal Representative:
SCHWEITZER Fritz L III, Schweitzer Cornman Gross & Bondell LLP, 230 Park Avenue, New York, NY 10163, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200056009 A1 20000921 (WO 0056009)
Application: WO 2000US7174 20000317 (PCT/WO US0007174)

Priority Application: US 99270874 19990317
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 27898

Fulltext Availability:
Detailed Description

Detailed Description
... we
further contemplate using such means to provide different access or use privileges to a **user** s portable electronic **device** or portable **storage medium** for different entities or programs or different **authorized** individuals. Note that this includes providing access to different services or functions, both in the...

23/3,K/53 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00743923 **Image available**
METHOD FOR SECURE POINT TO POINT COMMUNICATIONS
PROCEDE POUR COMMUNICATIONS POINT A POINT SECURISEES
Patent Applicant/Inventor:
PHILLIPS Geoff J, 3565 Caminito Carmel Landing, San Diego, CA 92130, US, US (Residence), US (Nationality)
Legal Representative:
GILLIAM Frank D, 4565 Ruffner St., Ste. 200, San Diego, CA 92111, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200057292 A1 20000928 (WO 0057292)
Application: WO 2000US7658 20000323 (PCT/WO US0007658)
Priority Application: US 99276475 19990325
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 2654

Fulltext Availability:
Detailed Description

Detailed Description
... other convenient storage medium can be used. The software requirements of the storage medium are **certification** , to "clone" (copy) data to the **diskette** from the **hard drive** for the guest **user** personal remote use and, "spawn"" (duplicate) to other diskettes from the hard drive or diskette...

23/3,K/52 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00749091 **Image available**

METHOD OF AND APPARATUS FOR PROVIDING SECURE COMMUNICATION OF DIGITAL DATA BETWEEN DEVICES

SECURISATION DES ECHANGES DE DONNEES NUMERIQUES ENTRE DISPOSITIFS ET APPAREIL A CET EFFET

Patent Applicant/Assignee:
CANAL+ SOCIETE ANONYME, 85/89, quai Andre Citroen, F-75711 Paris Cedex 15, FR, FR (Residence), FR (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:
MAILLARD Michel, 42, avenue du Marechal Leclerc, F-28130 Maintenon, FR, FR (Residence), FR (Nationality), (Designated only for: US)
DAUVOIS Jean-Luc, 19, rue Eugene Manuel, F-75116 Paris, FR, FR (Residence), FR (Nationality), (Designated only for: US)
DUBLANCHET Frederic, Canal+ Technologies Societe Anonyme, 34, place Raoul Dautry, F-75516 Paris Cedex 15, FR, FR (Residence), FR (Nationality), (Designated only for: US)
LEPORINI David, Canal+ Technologies Societe Anonyme, 34, place Raoul Dautry, F-75516 Paris Cedex 15, FR, FR (Residence), FR (Nationality), (Designated only for: US)

Legal Representative:
COZENS Paul Dennis, Mathys & Squire, 100 Gray's Inn Road, London WC1X 8AL, GB

Patent and Priority Information (Country, Number, Date):
Patent: WO 200062540 A1 20001019 (WO 0062540)
Application: WO 2000IB432 20000331 (PCT/WO IB0000432)
Priority Application: EP 99400901 19990413

Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 12524

Fulltext Availability:
Detailed Description

Detailed Description
... validation procedure can be initiated at any time, for example, upon switching the device on, **disc** insertion, zapping of the **device** by the **user** , establishment of connection with the security module etc.

The **validation** procedure is initiated by the security module. As shown at 100, the security module 64...

23/3,K/47 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00855226 **Image available**
SECURITY DEVICE AND ARTICLE INCORPORATING SAME
DISPOSITIF DE SECURITE ET ARTICLE COMPRENANT UN TEL DISPOSITIF
Patent Applicant/Assignee:
3LFANTS LIMITED, 19 Abbots Close, Knowle, Solihull, West Midlands B93 9PP , GB, GB (Residence), GB (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
CONSTANTINOU Andreas Sotiriou, 19 Abbots Close, Knowle, Solihull, West Midlands B93 9PP, GB, GB (Residence), GB (Nationality), (Designated only for: US)
SOTIRIOU Marios Panikos, 2 High Trees Road, Knowle, Solihull, West Midlands B93 9PR, GB, GB (Residence), GB (Nationality), (Designated only for: US)
DAVIES Guy, 52 Clopton Road, Stratford-Upon-Avon, Warwickshire CV37 6SN, GB, GB (Residence), GB (Nationality), (Designated only for: US)
Legal Representative:
MOSEY Stephen George (et al) (agent), Marks & Clerk, Alpha Tower, Suffolk Street, Queensway, Birmingham B1 1TT, GB,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200188921 A1 20011122 (WO 0188921)
Application: WO 2001GB2261 20010518 (PCT/WO GB0102261)
Priority Application: GB 200011904 20000518; GB 200024859 20001011
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 5722

English Abstract
A compact **disc** (10) for a **computer** incorporates a security **device** for preventing non- **authorised** reading of data carried by the disc. The security device includes an LCD laser blocker...

23/3,K/29 (Item 29 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00860521
Device and method for authenticating user's access rights to resources according to the Challenge-Response principle
Vorrichtung und Verfahren zur Authentifizierung von Zugangsrechten eines Benutzers zu Betriebsmitteln nach dem Challenge-Response-Prinzip
Dispositif et procede d'authentification de droits d'acces d'un utilisateur a des ressources selon le principe Challenge-Response
PATENT ASSIGNEE:
FUJI XEROX CO., LTD., (450442), 17-22, Akasaka 2-chome, Minato-ku, Tokyo, (JP), (Proprietor designated states: all)
INVENTOR:
Shin, Kil-ho, c/o Fuji Xerox Co., Ltd., 430 Sakai, Nakai-machi, Ashigarakami-gun, Kanagawa, (JP)
Kobayashi, Kenichi, c/o Fuji Xerox Co., Ltd., 430 Sakai, Nakai-machi, Ashigarakami-gun, Kanagawa, (JP)
Aratani, Toru, c/o Fuji Xerox Co., Ltd., 430 Sakai, Nakai-machi, Ashigarakami-gun, Kanagawa, (JP)
LEGAL REPRESENTATIVE:
Hoffmann, Eckart, Dipl.-Ing. (5571), Patentanwalt, Bahnhofstrasse 103, 82166 Grafelfing, (DE)
PATENT (CC, No, Kind, Date): EP 792044 A2 970827 (Basic)
EP 792044 A3 980527
EP 792044 B1 010502
APPLICATION (CC, No, Date): EP 97102779 970220;
PRIORITY (CC, No, Date): JP 9662076 960223; JP 97418 970106
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS (V7): H04L-009/32; G06F-001/00
ABSTRACT WORD COUNT: 157
NOTE:
Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199708W4	5228
CLAIMS B	(English)	200118	4877
CLAIMS B	(German)	200118	4269
CLAIMS B	(French)	200118	5603
SPEC A	(English)	199708W4	12074
SPEC B	(English)	200118	11928
Total word count - document A			17305
Total word count - document B			26677
Total word count - documents A + B			43982

...CLAIMS power of challenging data C stored in the first memory means 111 modulo n (R = **CD**)) mod n).
21. The **device** for **authenticating** user 's access rights to resources of claim 20, wherein
the response generation means 116 further...power of challenging data C stored in the first memory means 111 modulo n (R = **CD**)) mod n).
24. The **device** for **authenticating** **user** 's access rights to resources of claim 23, wherein
the response generation means 116 further...

...power of challenging data C stored in the first memory means 411 modulo p (R = **CD**)) mod p).
29. The **device** for **authenticating** **user** 's access rights to resources

of claim 28, wherein
the response generation means 416 further...

...CLAIMS challenging data C stored in the first memory means (111) modulo n, i.e. R = **CD**) mod n.

21. The **device** for **authenticating** **user** 's access rights to resources of claim 20, wherein

the response generation means (116) further...challenging data C stored in the first memory means (111) modulo n, i.e. R = **CD**) mod n.

24. The **device** for **authenticating** **user** 's access rights to resources of claim 23, wherein

the response generation means (116) further...

...challenging data C stored in the first memory means (411) modulo p, i.e. R = **CD**) mod p.

29. The **device** for **authenticating** **user** 's access rights to resources of claim 28, wherein

the response generation means (416) further...

. . .

. . .

23/3,K/27 (Item 27 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00999162
Authentication apparatus , user authentication **method,** user authentication **card and** storage medium
Authentifizierungsvorrichtung, Benutzerauthentifizierungsverfahren, Benutzerauthentifizierungskarte und Datentrager
Dispositif d'authentification, procede d'authentification d'utilisateur, carte d'authentification d'utilisateur et support de donnees
PATENT ASSIGNEE:
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku Kawasaki-shi,, Kanagawa 211-8588, (JP), (Applicant designated States: all)
INVENTOR:
Kubo, Takeshi, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
Igarashi, Kazuhiro, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
Saso, Hideyuki, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
LEGAL REPRESENTATIVE:
Dendorfer, Claus et al (85562), Wachtershauser & Hartz Weinstrasse 8, 80333 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 902352 A2 990317 (Basic)
EP 902352 A3 050928
APPLICATION (CC, No, Date): EP 98304268 980529;
PRIORITY (CC, No, Date): JP 97264839 970910; JP 9894592 980407
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-001/00
ABSTRACT WORD COUNT: 55
NOTE:
Figure number on first page: 6A 6B

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9911	2744
SPEC A	(English)	9911	19905
Total word count - document A			22649
Total word count - document B			0
Total word count - documents A + B			22649

Authentication apparatus , user authentication **method,** user authentication **card and** storage medium

SPECIFICATION
BACKGROUND OF THE INVENTION
The present invention generally relates to **authentication apparatuses** , **user authentication** methods, **user authentication** cards and **storage mediums** , and more particularly to an **authentication** apparatus, a user **authentication** method for an **authentication apparatus** , a **user authentication** card, and a **storage medium** storing a program for user **authentication** .
Conventionally, the security function provided in a personal computer (PC) generally carries out the authentication...

. . .

. . .

...it is a general object of the present invention to provide a novel and useful **authentication apparatus** , **user authentication** method, **user authentication** card and **storage medium** , in which the problems described above are eliminated.

Another and more specific object of the...

23/3,K/23 (Item 23 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01202670
Method of and apparatus for providing secure communication of digital data between devices
Verfahren und Anlage zur sicheren Ubertragung digitaler Daten zwischen Vorrichtungen
Procede et appareil pour transmettre en securite des donnees numeriques entre installations
PATENT ASSIGNEE:
CANAL+ Societe Anonyme, (1452151), 85/89 Quai Andre Citroen, 75711 Paris Cedex 15, (FR), (Applicant designated States: all)
INVENTOR:
Maillard, Michel, 42, Avenue du Marechal Leclerc, 28130 Maintenon, (FR)
Dauvois, Jean-Luc, 19 rue Eugene Manuel, 75116 Paris, (FR)
Dublanchet, Frederic, c/o Canal+Technologies S.A.,, 34 Place Raoul Dautry , 75516 Paris Cedex 15, (FR)
Leporini, David, c/o Canal+Technologies S.A.,, 34 Place Raoul Dautry, 75516 Paris Cedex 15, (FR)
LEGAL REPRESENTATIVE:
Cozens, Paul Dennis et al (72971), Mathys & Squire 100 Grays Inn Road, London WC1X 8AL, (GB)
PATENT (CC, No, Kind, Date): EP 1045585 A1 001018 (Basic)
APPLICATION (CC, No, Date): EP 99400901 990413;
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04N-005/913
ABSTRACT WORD COUNT: 48
NOTE:
Figure number on first page: 5

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200042	1858
SPEC A	(English)	200042	8933
Total word count - document A			10791
Total word count - document B			0
Total word count - documents A + B			10791

...SPECIFICATION validation procedure can be initiated at any time, for example, upon switching the device on, **disc** insertion, zapping of the **device** by the **user** , establishment of connection with the security module etc.

The **validation** procedure is initiated by the security module. As shown at 100, the security module 64...

23/3,K/22 (Item 22 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01215702
Fully lazy linking with module-by-module verification
Sehr langsame Verknupfung wobei Modul nach Modul Uberpruft wird
Edition de liens completement paresseuse en verifiant module apres module
PATENT ASSIGNEE:
SUN MICROSYSTEMS, INC., (1392733), 901 San Antonio Road, Palo Alto, California 94303, (US), (Applicant designated States: all)
INVENTOR:
Bracha, Gilad, 2042 Farndon Avenue, Los Altos, CA 94024, (US)
Liang, Sheng, 10440 Oakville Avenue, Cupertino, CA 95014, (US)
Lindholm, Timothy G., 623 Middlefileld Road, Palo Alto, CA 94301, (US)
LEGAL REPRESENTATIVE:
Walaski, Jan Filip et al (92081), Venner, Shipley & Co, 20 Little Britain , London EC1A 7DH, (GB)
PATENT (CC, No, Kind, Date): EP 1056002 A2 001129 (Basic)
EP 1056002 A3 011212
APPLICATION (CC, No, Date): EP 2000304310 000522;
PRIORITY (CC, No, Date): US 321226 990527
DESIGNATED STATES: DE; FR; GB; IE; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-009/445; G06F-011/00
ABSTRACT WORD COUNT: 95
NOTE:
Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200048	863
SPEC A	(English)	200048	12726
Total word count - document A			13589
Total word count - document B			0
Total word count - documents A + B			13589

...CLAIMS a constrained module after said retaining, until all pre-verification constraints are read.
5. A **verification** apparatus for **verifying** a module during linking, the **apparatus** comprising:
a **computer** readable **storage medium** for storing a module of a computer program;
a memory into which a module is...

23/3,K/21 (Item 21 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01215703
Module-by-module verification
Uberprufung von Modul nach Modul
Verifier module apres module
PATENT ASSIGNEE:
SUN MICROSYSTEMS, INC., (1392733), 901 San Antonio Road, Palo Alto, California 94303, (US), (Applicant designated States: all)
INVENTOR:
Bracha, Gilad, 2042 Farndon Avenue, Los Altos CA 94024, (US)
Liang, Shenh, 10440 Oakville Avenue, Cupertino, CA 95014, (US)
Lindholm, Timothy G., 623 Middlefield Road, Palo Alto CA 94301, (US)
LEGAL REPRESENTATIVE:
Walaski, Jan Filip et al (92081), Venner, Shipley & Co, 20 Little Britain , London EC1A 7DH, (GB)
PATENT (CC, No, Kind, Date): EP 1056003 A2 001129 (Basic)
EP 1056003 A3 011212
APPLICATION (CC, No, Date): EP 2000304311 000522;
PRIORITY (CC, No, Date): US 320574 990527
DESIGNATED STATES: DE; FR; GB; IE; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-009/445; G06F-011/00
ABSTRACT WORD COUNT: 122
NOTE:
Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200048	1656
SPEC A	(English)	200048	12803
Total word count - document A			14459
Total word count - document B			0
Total word count - documents A + B			14459

...CLAIMS constraints are read, whereby the first module is verified.
17. A pre-verification apparatus for **verifying** a module one-module-at-a-time, the **apparatus** comprising:
a **computer** readable **storage medium** for storing a module of a computer program and a constraint;
a processor configured to...

...an error message if the instruction fails to satisfy any intra-module check.
20. A **verification** apparatus for **verifying** a module during linking, the **apparatus** comprising:
a **computer** readable **storage medium** for storing a module of a computer program;
a memory into which a module is...

. . .

. . .

23/3,K/19 (Item 19 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01215706
Trusted verification of computer program modules
Vertraute Uberprufung von Rechnerprogrammmodulen
Verification securisee des modules de programme d'ordinateur
PATENT ASSIGNEE:
SUN MICROSYSTEMS, INC., (1392733), 901 San Antonio Road, Palo Alto, California 94303, (US), (Proprietor designated states: all)
INVENTOR:
Bracha, Gilad, 2042 Farndon Avenue, Los Altos, CA 94024, (US)
Liang, Sheng, 10440 Oakville Avenue, Cupertino, CA 95014, (US)
Lindholm, Timothy G., 623 Middlefield Road, Palo Alto, CA 94301, (US)
LEGAL REPRESENTATIVE:
Walaski, Jan Filip et al (92081), Venner Shipley LLP 20 Little Britain, London EC1A 7DH, (GB)
PATENT (CC, No, Kind, Date): EP 1056013 A2 001129 (Basic)
EP 1056013 A3 010829
EP 1056013 B1 050309
APPLICATION (CC, No, Date): EP 2000304319 000522;
PRIORITY (CC, No, Date): US 320581 990527
DESIGNATED STATES: DE; FR; GB; IE; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-011/36
ABSTRACT WORD COUNT: 76
NOTE:
Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200048	1851
CLAIMS B	(English)	200510	1047
CLAIMS B	(German)	200510	1156
CLAIMS B	(French)	200510	1300
SPEC A	(English)	200048	12930
SPEC B	(English)	200510	12564
Total word count - document A			14784
Total word count - document B			16067
Total word count - documents A + B			30851

...CLAIMS the referenced module, if the information is required.
18. A dynamic linking apparatus for trusted **verification** of a module during dynamic linking, the **apparatus** comprising:
a **computer** readable **storage medium** for storing a module of a computer program;
a memory into which a module is...

23/3,K/16 (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01295846
SYSTEM FOR CONTROLLING INFORMATION ON CONDITION OF CONTENTS USE
SYSTEM ZUM KONTROLLIEREN VON INFORMATION UNTER AUFLAGE VON INHALTSVERWENDUNG
SYSTEME DE CONTROLE D'INFORMATION SUR LES CONDITIONS D'UTILISATION DE CONTENU
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
Ishiguro, Ryuji Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001, (JP)
Kawakami, Itaru Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001, (JP)
Tanabe, Mitsuru Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001, (JP)
Ezura, Yuichi Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001, (JP)
Sato, Ichiro Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001, (JP)
Ebihara, Munetake Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Melzer, Wolfgang, Dipl.-Ing. et al (8278), Patentanwalte Mitscherlich & Partner, Sonnenstrasse 33, 80331 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1158418 A1 011128 (Basic)
WO 200131462 010503
APPLICATION (CC, No, Date): EP 2000970074 001025; WO 2000JP7474 001025
PRIORITY (CC, No, Date): JP 99303140 991025
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-015/00; G06K-015/02
ABSTRACT WORD COUNT: 38

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200148 2050
SPEC A (English) 200148 17963
Total word count - document A 20013
Total word count - document B 0
Total word count - documents A + B 20013
...SPECIFICATION memory card loaded on the portable device (X) 6-3 are transferred to the hard **disc** 21 on the personal **computer** 1.
The portable **device** (X) 6-3 holds ID information (MG-ID), **authentication** keys (MG-IK) for plural generations and master keys (OMG-MK) for plural generations from..

. . .

. . .

23/3,K/14 (Item 14 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01300940
METHOD FOR MANAGING CONTENT DATA
VERFAHREN ZUM VERWALTEN VON INHALTS-DATEN
PROCEDE DE GESTION DE DONNEES DE CONTENU
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
ISHIGURO, Ryuji, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
KAWAKAMI, Itaru, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
TANABE, Mitsuru, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
EZURA, Yuichi, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
SATO, Ichiro, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
EBIHARA, Munetake, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Melzer, Wolfgang, Dipl.-Ing. (8278), Patentanwalte Mitscherlich & Partner, Sonnenstrasse 33, 80331 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1158416 A1 011128 (Basic)
WO 200135236 010517
APPLICATION (CC, No, Date): EP 2000970072 001025; WO 2000JP7472 001025
PRIORITY (CC, No, Date): JP 99303139 991025; JP 99303141 991025
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-015/00; G06F-017/60; G06F-013/00; G10K-015/02
ABSTRACT WORD COUNT: 126

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200148 1374
SPEC A (English) 200148 18880
Total word count - document A 20254
Total word count - document B 0
Total word count - documents A + B 20254
...SPECIFICATION memory card loaded on the portable device (X) 6-3 are transferred to the hard **disc** 21 on the personal **computer** 1.
The portable **device** (X) 6-3 holds ID information (MG-ID), **authentication** keys (MG-IK) for plural generations and master keys (OMG-MK) for plural generations from...

23/3,K/11 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01322557
Distributed cryptography technique for protecting removable data storage media
Verteiltes kriptographisches Verfahren zur Sicherung von abnehmbaren Datenspeichermedien
Technique cryptographique pour la protection des supports de donnees amovibles
PATENT ASSIGNEE:
IOMEGA CORPORATION, (482102), 1821 West 4000 South, Roy, UT 84067, (US), (Applicant designated States: all)
INVENTOR:
Thomas, Fred C., III, 2491 Woodland Drive, Ogden, Utah 84403, (US)
Watson, Brent, 1263 East Beverly, Bountiful, Utah 84010, (US)
Fowler, Steven M., 2095 South Main Street, No. 22, Bountiful, Utah 84010, (US)
Bero, James M., 4207 Skyline Drive, Ogden, Utah 84403, (US)
Taylor, Wilhelm, 1665 Beechwood Drive, Layton, Utah 84040, (US)
LEGAL REPRESENTATIVE:
Cabinet Hirsch (101611), 34, Rue de Bassano, 75008 Paris, (FR)
PATENT (CC, No, Kind, Date): EP 1130494 A2 010905 (Basic)
APPLICATION (CC, No, Date): EP 2000403668 001222;
PRIORITY (CC, No, Date): US 176087 P 000114; US 565790 000505
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-001/00
ABSTRACT WORD COUNT: 191
NOTE:
Figure number on first page: 4

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200136	973
SPEC A	(English)	200136	7397
Total word count - document A			8370
Total word count - document B			0
Total word count - documents A + B			8370

...SPECIFICATION component and a second component. Components, e.g., can include a host, a data storage **device** , a **user authentication device** , a **user** , a **client** application, a data **storage medium** , and the like. The respective components of each computer system are substantially similar i.e...in a computer system by distributing cryptographic information for cryptographically securing data transferred to a **storage medium** . Enterprise user 300, host 90, **user authentication device** 330, removable data storage device 50 and removable data storage medium 360, e.g., each...

```
S33        330   S5(10N)S1(10N)S9(10N)(S2 OR SERVER?)
S34          0   S33 AND S28(10N)S2
S35         34   S33 AND S28 AND S2
S36         32   S33 AND S3
S37         77   S33 AND S28
S38         12   S37 AND S3
S39         54   S35:S36
S40        151   S14:S16 OR S18:S23
S41         32   S39 NOT S40
S42         40   S37 NOT S40:S41
S43         72   S41:S42
S44         29   S43 NOT AD=2002:2006
S45          9   S38 NOT AD=2002:2006
S46         38   S44:S45
S47         38   IDPAT (sorted in duplicate/non-duplicate order)
File 348:EUROPEAN PATENTS 1978-2006/Feb W04
         (c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060302,UT=20060223
         (c) 2006 WIPO/Univentio
```

47/3,K/16 (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01276898
CONTENTS MANAGEMENT SYSTEM, DEVICE, METHOD, AND PROGRAM STORAGE MEDIUM
INHALTSVERWALTUNGSSYSTEM, VORRICHTUNG, VERFAHREN UND PROGRAMMSPEICHERMEDIUM
SYSTEME, DISPOSITIF, PROCEDE ET SUPPORT DE PROGRAMME POUR LA GESTION DE CONTENUS

PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
ISHIBASHI, Yoshihito, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
OHISHI, Tateo, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
MUTO, Akihiro, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
KITAHARA, Jun, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
SHIRAI, Taizou, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
DeVile, Jonathan Mark, Dr. et al (91151), D. Young & Co 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1128598 A1 010829 (Basic)
WO 200119017 010315
APPLICATION (CC, No, Date): EP 2000956997 000907; WO 2000JP6089 000907
PRIORITY (CC, No, Date): JP 99253660 990907; JP 99253661 990907; JP 99253662 990907; JP 99253663 990907; JP 99260638 990914; JP 99264082 990917; JP 99265866 990920
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04L-009/32; G06F-015/00; H04N-005/91; G11B-020/10; G10K-015/04; H04N-007/167
ABSTRACT WORD COUNT: 172
NOTE:
Figure number on first page: 0020

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200135	29406
SPEC A	(English)	200135	83907
Total word count - document A			113313
Total word count - document B			0
Total word count - documents A + B			113313

...SPECIFICATION and thus a recording and reproducing apparatus, a recording and reproducing method and a program **storage medium** capable of markedly improving versatility of data storage apparatuses can be implemented.

In addition, the...apparatus, and thus a data storage apparatus, a data management and migration method and aprogram **storage medium** that allow contents data recorded on a data storage apparatus to be easily utilized by...

...regulating apparatus.

Thus, an information receiving apparatus, a data utilization method and a program storage **medium** capable of, by having an information

regulating apparatus determine in advance whether received contents data ...

...showing the received contents data by an information receiving apparatus, and prohibiting utilization, that is, **verifying** a signature on utilization permission data to determine whether the utilization permission data is illegal...in the case where a home server charges.

Figure 90 is a flowchart showing a **proxy** purchasing procedure in the case where equipment outside the group charges.

Figure 91 is a...but no specific hardware limitation is necessary. (For example, the memory may be a hard **disk** existing in a room to which entry is managed, a hard **disk** of a personal computer that is managed by a password, or the like.) In addition...

...a memory 40B only stores the individual key Ki)) that is encrypted by the delivery **key** Kd)) and the public **key** **certificate** of the content provider 2, the memory may be any ordinary storage device or the...

...40A and 40B may be united.

The signature, which is attached to data or a **certificate** to be described later, is data for checking tamper and authenticating a person preparing the...be kept secret is called a secret key.

The elliptic curve encryption method that is **representative** of the public **key** encryption method will be described. In Figure 12, in step S20, Mx)) and My)) are...watermark technology to output to other apparatuses or a speaker (not shown), and reproduces music.

Key data required for the mutual **authentication** with the encryption processing section 65 is stored in the storage module 106. Further, the...

...the save key Ksave)). The mass storage section 68 records the secure container, the public **key** **certificate** , the registration information or the like supplied from the service provider 3.

The fixed apparatus...

...from the service provider 3 in an inserted recording medium 80 such as an optical **disk** and a semiconductor memory and reproducing the recording media is composed of a communication section...

...as the mass storage section 68, contents themselves are not stored and only the public **key** **certificate** , the registration information or the like are stored. The record reproduction section 76 has the recording medium 80 such as an optical **disk** and a semiconductor memory inserted therein, records contents in the recording medium 80 and output...67, its description is omitted. The recording medium 80 is, for example, an MD (Mini **Disk** : trademark) or a storage medium exclusively used for electronic distribution (Memory Stick using a semiconductor...

...the public key of the electronic distribution service center 1 to be used when mutually **authenticating** with the electronic distribution service center 1 (unnecessary if there is the public key certificate...
...the electronic distribution service center 1), the public key of the authentication station 22 for **verifying** the public **key** **certificate** , and the common **key** to be used when mutually **authenticating** with the extension section 66 are stored in the storage module 92 in the encryption...

...the storage module 92. The individual ID for specifying the extension section and the common **key** to be used when mutually **authenticating** with the encryption processing section 65 are stored in the storage module 106 in the...

...one, IDs of each section may be held by respective storage modules (since the mutual **authentication** is performed by the common **key** , as a result, communication can only be made between the corresponding encryption processing section and the extension section associated with each other. However, processing may be the mutual **authentication** of the public **key** encryption method. In this case, a stored key is not the common key, but the...

...utilizing the content key Kco)) are stored in the external memory 67. In addition, the **certificate** (the public key certificate of an apparatus) of the public key corresponding to the secret...
...all the procedures with the electronic distribution service center 1 on its behalf), the public **key** of the **authentication** station 22 for **verifying** the public **key certificate** , and the common **key** to be used when mutually **authenticating** with the extension section 84 are stored. These data are data that are stored in...secure container, the public key certificate of the content provider 2, and the public key **certificate** of the service provider 3 (whose details will be described later) are transmitted to the...

...addition, the service provider 3 transmits the price information and its signature, and the public **key certificate** of the service provider 3 to the electronic distribution service center 1, if necessary.

After **verifying** the received secure containers, the user home network 5 performs the purchase processing based on...

...the save key Ksave)), and stores the license conditions information and the re-encrypted content **key** Kco)) in the external memory 67. Then, the user home network 5 decodes the content...hash value generated by applying a hash function to a version number of the public **key certificate** , a serial number of the public **key certificate** to be allocated to the content provider 2 by the **authentication** station, an algorithm and a parameter used for the signature, a name of the **authentication** station, an effective period of the public **key certificate** , a name of the content provider 2, the public key Kpcp)) of the content provider...

...encrypted by the delivery key Kd)).

Figure 28 illustrates yet another example of the public **key certificate** of the content provider 2. The public key certificate 2B of the content provider 2...

...the signature, a name of the authentication station, an effective period of the public key **certificate** , a name of the content provider 2, the public key Kpcp)) of the content provider...rules, the rules stored in the position indicated by the address information, the public key **certificate** and signatures.

The rule is composed of a rule number given as a serial number...

...the rules, the rules stored in the position indicated by the address information, the public **key certificate** and signatures.

Further, similar to the rule of the handling policy of the single content...signature is affixed to the entirety ranging from a type of data to a public **key certificate** excluding the signature from a handling policy. An algorithm and a parameter used in preparing the signature and a **key** to be used for **verification** of the signature are included in the public **key certificate** . In addition, in rules, a utilization right content number is a number added for each... authenticates with the mutual authentication section 39 of the content

provider 2. Since the mutual **authentication** processing was described in Figure 52, its details are omitted. When it is confirmed that...

...management section 18 of the electronic distribution service center 1. In step S60, the home **server** 51 mutually **authenticates** a public **key certificate** stored in the mass storage section 68 with the mutual **authentication** section 17 of the electronic distribution service center 1 in the mutual **authentication** module 95 of the encryption processing section 65. Since this **authentication** processing is similar to that described with reference to Figure 52, description is omitted here. A **certificate** that the home **server** 51 transmits to the user management section 18 of the electronic distribution service center 1 in step S60 includes data (a public **key certificate** of a user apparatus) shown in Figure 32.

In step S61, the home **server** decides whether or not a registration of an individual's settlement information (such as a...and the signature verification of the individual key Ki)) (step S455) as well as the **substitute** processing of the content **key** Kco)) that have already been performed in the purchase processing described with reference to Figure ...

47/3,K/27 (Item 27 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00848565 **Image available**
METHODS AND SYSTEMS FOR SECURING COMPUTER SOFTWARE
PROCEDES ET SYSTEMES POUR SECURISER UN LOGICIEL INFORMATIQUE
Patent Applicant/Assignee:
VENICE TECHNOLOGIES INC, 18 Russell Street, Brookline, MA 02446-2414, US, US (Residence), US (Nationality)
Inventor(s):
HERLIHY Maurice, 18 Russell Street, Brookline, MA 02446-2414, US,
Legal Representative:
POWSNER David J (et al) (agent), Nutter, McClennen & Fish LLP, One International Place, Boston, MA 02110-2699, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200182204 A1 20011101 (WO 0182204)
Application: WO 2001US13792 20010426 (PCT/WO US0113792)
Priority Application: US 2000199934 20000426; US 2000199935 20000426; US 2000200156 20000426; US 2000207560 20000525; US 2000207559 20000525
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 8538

Fulltext Availability:
Detailed Description

Detailed Description
... processing devices, from PDAs to video game boards. The client program is transferred to the **client device** 109 via install **disks** , downloading, or any other mechanism known in the art for code transfer and installation. Further...for distribution of both the client prograni and server tables (and possibly parts of the **server** program) to the client site on **CD** , DVI) or other computer readable media, for example. The security of the transforination relies on ensuring that an unauthorized user never obtains access to the **server** tables. One can achieve this goal by keeping the tables encrypted where the encryption **key** is known orily to **authorized servers** . The **vendor** splits the original program into a process and **server** with an encrypted set of **server** tables, where the encryption **key** is known only to the **vendor** . In order to execute the client, it sends the encrypted tables to a **server** , where they are decrypted and. used by the server until such time as the client...

47/3,K/28 (Item 28 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00846298 **Image available**
METHOD AND SYSTEM FOR DELIVERY AND EXECUTION OF COPY PROTECTED DIGITAL CONTENT
PROCEDE ET SYSTEME DE DISTRIBUTION ET D'EXECUTION DE CONTENU NUMERIQUE PROTEGE CONTRE LA COPIE

Patent Applicant/Assignee:
IOMEGA CORPORATION, 1821 West Iomega Way, Roy, UT 84067, US, US (Residence), US (Nationality)
Inventor(s):
HALES Ronald F, 4052 S. 950 W., Riverdale, UT 84405, US,
ISAACSON Shawn R, 4360 S. 2175 S., Roy, UT 84067, US,
SHORT Robert, 7714 Crestview Drive, Niwot, CO 80501, US,
PETERS Eric, 4099 W. 5600 S., Roy, UT 84067, US,
ADAMS Chad, 5299 S. 2690 W., Roy, UT 84067, US,
Legal Representative:
BUTTER Gary M (agent), Baker Botts LLP, 30 Rockefeller Plaza, New York, NY 10112-0228, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200179972 A2-A3 20011025 (WO 0179972)
Application: WO 2001US40471 20010409 (PCT/WO US0140471)
Priority Application: US 2000551098 20000418; US 2000602218 20000623; US 2000602219 20000623
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS
LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ
TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 16444

Fulltext Availability:
Detailed Description

Detailed Description
... playback hardware device such as a compact disk player or an MP3 player. If the **hardware** or **computer** associated with the removable **storage medium** 38 has content player software or finnware, the content 60 is decrypted and played as...4168. Data encryption occurs via a 16-round Feistel network. Each round consists of a **key** -dependent permutation and a datadependent **substitution** . All operations are XORs ((inverted exclamation mark).e., exclusive or) and additions on 32-bit... content player uses the device type bits to detennine from what device and thus data **storage medium** 38 to query for the unique ID code incorporated in the Blowfish eneryption key in order to unlock the Blowf(inverted exclamation mark)sh-encrypted **authentication** string and XOR file **key** stored in the **authentication** descriptor 304. The download **server** software 312 sets these bits prior to downloading content 60, in this instalice music, to...

...typically used.

0= removable type (e.g. lomega removable type)
1= hard drive type
2= **CD** type
3= other type (e.g. flash memory, etc...

The file type field contains an...encrypted using the random, S-byte (64-bit) XOR file key selected by the downIoad **server** software 312. The XOR file key is also encrypted, using the Blowfish algorithm with the encryption key being the unique ID code of the data **storage medium** 38. Once the XOR file key is encrypted, the download **server** software 312 embeds the XOR **key** in the **authentication** descriptor for the content player such as the client computer 20, the dedicated playback hardware...

47/3,K/29 (Item 29 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00841904 **Image available**
DIGITAL RIGHTS MANAGEMENT WITHIN AN EMBEDDED STORAGE DEVICE
GESTION NUMERIQUE DE DROITS DANS UN DISPOSITIF DE MEMOIRE INTEGRE
Patent Applicant/Assignee:
DATAPLAY INC, 2560 55th Street, Boulder, CO 80301-5706, US, US (Residence), US (Nationality)
Inventor(s):
LEE Lane W, 894 S. Bermont Drive, Lafayette, CO 80026, US,
ZAHARRIS Daniel R, 7329 Mt. Meeker Road, Longmont, CO 80503, US,
Legal Representative:
STEUBER David E (et al) (agent), Skjerven Morrill MacPherson LLP, 25 Metro Drive, Suite 700, San Jose, CA 95110, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200175562 A2-A3 20011011 (WO 0175562)
Application: WO 2001US10405 20010329 (PCT/WO US0110405)
Priority Application: US 2000542510 20000403
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9881

Fulltext Availability:
Detailed Description

Detailed Description
... data stored on a storage medium.

An engine for reading the data stored on the **storage medium** is connected to a host **device** . A **user** of the **storage medium** selects a portion of the data on the storage ...places a new storage medium in data storage engine 14, or if the 1 5 **user** powers up host **device** 12 with a **storage medium** (e.g. an optical disk) in data storage engine 14. In stage 205, the host device reads the content infon-nation block from **storage medium** 1 0 and displays the content information block to the user. In stage 210, host...

...the user's selection of data to enable. Host device 12 then connects to content **key server** 17 or a distributor **authorization server** and satisfies the requirements of the distributor for the selected data in stage 210. Host...

...both handled by a single server, content key server 17. Thus, there is no separate **vendor authorization** server. Content **key** server 17 includes application programs 17A, data access server 17B, and web server 17C. Application...be unlocked. The content selected by the user may be all the data stored on **storage medium** 1 0, or only a portion of the

data stored on **storage medium** 10. The message **authorization** code (MAC) 32 is a encrypted hash of the entire packet that **verifies** content **key server** 17 that the packet has not been altered in transit. Session ID 33 is generated by content key **server** 17 and sent to data storage engine 14 when the user requests pricing information in...

...indicates whether data storage engine 14 was able to successfully store the content key on **storage medium** 10. If pass/fail indicator 41 indicates that data storage 1 5 engine 14 was...
...store the content key, the transaction required by the distributor between the user and content **key server** 17 or the distributor **authorization server** is canceled. Packet ID 39 is generated by data storage engine 14.

In one embodiment, the **server certificate** , random challenge, and public/private **key** used to encrypt the three information packets, pairs are generated using a toolkit called "Security...464, the decrypted packet is separated into the packet formed in stage 430 and the **server** signature formed in stage 432. In stage 466, the packet formed in stage 430 is separated into the random challenge, the server **certificate** , the encrypted server t-DES **key** set, and the data packet fon-ned in stage 424. In stage 468, the server **certificate** is **verified** using the manufacturer's public **key** , part of the public/private manufacturer key pair, which is given to the engine during...

...digital signature on the packet formed in stage 430 and signed in stage 432 is **verified** using the server public **key** , part of the public/private server key pair, which is contained within the server **certificate** .

In stage 472, the **server** t-DES key set formed in stage 426 is decrypted using the private engine key...

...during manufacture. In stage 474, the packet formed in stage 424 is decrypted using the **server** t-DES key set. The decrypted information can then be separated and the content keys...

...each file enabled by the user retrieved. The content keys are then written to the **storage medium** by the data storage engine. The keys may be encrypted using a secret key stored...The
each message digest for the signature is
licensed created through the SHA- I hash
server function.

Verify Engine ecdsa- **Verify** Public **Key** , This function **verifies** that a signature Signed is authentic.

Message
Digest
Encrypt Server sb-desEncrypt TDES-CBC Used...

...TDES-CBC encryption.
Initial
Vector, Data
Decrypt Server sb-desDecrypt TDES-CBC Used by the **server** to decrypt the data mode, Keys, using TDES-CBC mode.

Initial
Vector, Data
Decrypt Engine...

...a hardware ASIC to
ASIC mode, Keys, perform TDES-CBC decryption.

Initial
Vector, Data
Wrap **Server** sb
.ecesWrap Public Key, Encrypts data using using a 326-bit
Data ECC public key...

...private key.

CreateMac Engine Hardware Data, Key Creates the MAC used as hash and
ASIC **authentication** for the engine.
CreateMac **Server** sb-desEncrypt Data, **Key** Creates the MAC used to
verify the MAC created by the engine.

Various modifications and adaptations of the embodiments and
implementations...

...of data required to read the data or make sense of the data stored on
storage medium 10. Specifically, in some embodiments, the data stored
on the storage medium is not encrypted...

47/3,K/37 (Item 37 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00376053 **Image available**
SYSTEM FOR CUSTOMIZED ELECTRONIC IDENTIFICATION OF DESIRABLE OBJECTS
SYSTEME DE REPERAGE ELECTRONIQUE PERSONNALISE D'OBJETS DE RECHERCHE
Patent Applicant/Assignee:
HERZ Frederick S M,
EISNER Jason M,
SMITH Jonathan M,
SALZBERG Steven L,
Inventor(s):
HERZ Frederick S M,
EISNER Jason M,
SMITH Jonathan M,
SALZBERG Steven L,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9716796 A1 19970509
Application: WO 96US17981 19961029 (PCT/WO US9617981)
Priority Application: US 95551198 19951031
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AM AU BR BY CA CN EE IL IS JP KP KR KZ LV MN MX NZ RU SG TM TR UA UZ VN
AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 51971

Fulltext Availability:
Detailed Description

Detailed Description
... contains a public key PKp, user-specific information, and credentials associated with pseudonym P. The **proxy** server S2 uses the public **key** PKp to check that the signed version S(R, SK) of request message R is...A summary of such relevance feedback information, digitally signed by client processor C3 with a **proprietary** private **key** SKC3, is periodically transmitted through an a secure mix path to the proxy server S2...by the user establishing a pseudonymous data communications connection as described above to a proxy **server** S2i which provides front-end access to the data communication network N. The proxy **server** S2 maintains a list of **authorized** pseudonyms and their corresponding public **keys** and provides access and billing control. The user has a search profile set stored in the local data **storage medium** on the proxy **server** S2. When the user requests access to "news" at step 1102, the profile matching module 203 resident on proxy **server** S2 sequentially considers each search profile Pk from the user's search profile set to...

```
Set     Items   Description
S1    1239329   STORAGE()(MEDIA? ? OR MEDIUM? ?) OR DVD OR DISK? OR DISC? ?
           OR CD OR CD()ROM OR TAPE? ? OR (DAT OR DIGITAL()ANALOG OR CA-
           SSETTE)()TAPE? ?
S2       2549   ((COMPUTER? OR CLIENT??? OR HANDHELD? OR USER? ? OR PDA OR
           PALM()PILOT? OR HANDSET? ? OR DESKTOP?? OR LAPTOP??)(3N)(DEVI-
           CE? OR INSTRUMENT? OR MECHANISM? OR MACHINE? ? OR UNIT? OR AP-
           PARAT? OR HARDWARE? OR (HARD OR CD OR DVD)()DRIVE?))(10N)S1
S3         10   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
           HORIZ? OR AUTHORIS? OR APPROV? OR VERIF?)(10N)S2
S4     936563   KEY???
S5      10373   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
           HORIZ? OR AUTHORIS? OR APPROV? OR VERIF?)(5N)S4
S6        715   (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
           DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
           OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?)(-
           7N)S5
S7          0   (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
           DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
           OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?)(-
           5N)(S1(7N)S5)
S8   13882355   RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR -
           DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
           OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?
S9    1676005   CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
           ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S10    139818   DECRYPT? OR DECIPHER? OR DECOD? OR UNSCRAMBL? OR DESCRAMBL?
S11      1047   (INTERMEDIAR? OR GO()BETWEEN? OR MIDDLEMAN OR PROXY OR BRO-
           KER? OR NEGOTIATOR? OR VENDOR?)(5N)S4:S5
S12      2743   (SURROGAT? OR EMISSAR? OR INTERCESSOR? OR MEDIATOR? OR INT-
           ERAGENT? OR FINANCIER? OR PROPRIET?)(5N)S4:S5
S13      4563   (AGENT? ? OR REPRESENTATIVE? OR ARBITRATOR? OR PROMOTER? OR
           MEDIAR? OR EXECUTOR? OR SUBSTITUT?)(5N)S4:S5
S14     69717   (EXCHANG? OR RECIPROC??? OR REVERS? OR MUTUAL? OR SWAP??? -
           OR SWAPS OR SWAPPING OR TRADE? ? OR TRADING OR SWITCH? OR TRA-
           NSACT?)(S7)(S4:S5)
S15         0   S5(10N)S1 AND S9 AND S2
S16         0   S2 AND S14 AND S11:S13
S17        59   S5 AND (S6 OR S14) AND S11:S13
S18         0   S17 AND S2 AND (S6 OR S14) AND S11:S13
S19     12942   STREAM???()(MEDIA()CONTENT? ? OR VIDEO??? OR AUDIO???) OR -
           (DELIVER??? OR SEND??? OR DOWNLOAD??? OR UPLOAD???)(3N)(REAL(-
           )TIME OR REALTIME OR LIVE OR IMMEDIAT? OR INSTANT? OR STREAM?-
           ?? OR UP(3W)(MINUTE? OR SECOND? OR MOMENT?))
S20      2954   (NETWORK? OR NET? ? OR INTERNET? OR INTRANET? OR ONLINE OR
           WAN? ? OR LAN? ? OR ETHERNET? OR EXTRANET? OR WWW OR WORLD()W-
           IDE()WEB OR WORLDWIDEWEB OR SUBNET? OR SERVER? ? OR WEB()SERV-
           ER? ?)(10N)S19
S21         0   S20 AND S6 AND S2
S22         0   S19 AND S6 AND S2
S23         9   S2 AND S14
S24         0   S2 AND S11:S13
S25         0   S2 AND S14 AND SERVER?
S26        12   S9(10N)S20
S27         0   S9 AND S20 AND S14 AND S2
S28       516   S1 AND S8:S10 AND S14
S29         4   S28 AND S2
S30        16   S26 OR S29
S31        16   S29:S30
S32         2   S28 AND S19:S20
S33     13895   AU=(CHAN S? OR CHAN, S?)
```

```
S34          0   AU=(MAYMUDES D? OR MAYMUDES, D?)
S35          0   SHANNON(2N)CHAN OR (DAVE OR DAVID)(2N)MAYMUDES
S36      13895   S33:S35
S37          7   S36 AND S20
S38          0   S37 AND (S4:S5 OR S14)
S39          0   S36 AND S2
S40          0   S36 AND S11:S13
File   2:INSPEC 1898-2006/Feb W4
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Feb W3
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Feb W4
         (c) 2006 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Feb W4
         (c) 2006 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2006/Feb
         (c) 2006 ProQuest Info&Learning
File  62:SPIN(R) 1975-2006/Feb W2
         (c) 2006 American Institute of Physics
File  65:Inside Conferences 1993-2006/Mar 09
         (c) 2006 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2006/Dec W2
         (c)2006 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2006/Mar W1
         (c) 2006 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Feb
         (c) 2006 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 02
         (c) 2006 The Gale Group
File 144:Pascal 1973-2006/Feb W2
         (c) 2006 INIST/CNRS
File 239:Mathsci 1940-2006/Apr
         (c) 2006 American Mathematical Society
File 256:TecInfoSource 82-2006/Feb
         (c) 2006 Info.Sources Inc
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
```

```
Set     Items   Description
S1    3210948   STORAGE()(MEDIA? ? OR MEDIUM? ?) OR DVD OR DISK? OR DISC? ?
               OR CD OR CD()ROM OR TAPE? ? OR (DAT OR DIGITAL()ANALOG OR CA-
               SSETTE)()TAPE? ?
S2      32176   ((COMPUTER? OR CLIENT??? OR HANDHELD? OR USER? ? OR PDA OR
               PALM()PILOT? OR HANDSET? ? OR DESKTOP?? OR LAPTOP??)(3N)(DEVI-
               CE? OR INSTRUMENT? OR MECHANISM? OR MACHINE? ? OR UNIT? OR AP-
               PARAT? OR HARDWARE? OR (HARD OR CD OR DVD)()DRIVE?))(10N)S1
S3        450   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
               HORIZ? OR AUTHORIS? OR APPROV? OR VERIF?)(10N)S2
S4    6605508   KEY???
S5      68455   (CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUT-
               HORIZ? OR AUTHORIS? OR APPROV? OR VERIF?)(5N)S4
S6     299549   (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
               DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
               OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?)(-
               7N)S4:S5
S7        925   (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
               DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
               OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?)(-
               5N)(S1(5N)S4:S5)
S8   26336829   RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR -
               DOWNLOAD? OR RECIPIEN??? OR FETCH??? OR TRANSFER? OR PASS??? -
               OR DELIVER??? OR SEND??? OR UPLOAD??? OR TRANSMIT? OR BEAM?
S9    8044805   CERTIFICAT? OR CERTIF? OR AUTHENTICAT? OR VALIDAT? OR AUTH-
               ORIZ? OR AUTHORIS? OR APPROV? OR VERIF?
S10    186234   (EXCHANG? OR RECIPROC??? OR REVERS? OR MUTUAL? OR SWAP??? -
               OR SWAPS OR SWAPPING OR TRADE? ? OR TRADING OR SWITCH? OR TRA-
               NSACT?)(5N)(S4:S5)
S11         1   (S1(5N)S4:S5)(5N)S3
S12       314   S1 AND S1(5N)S10
S13        16   S12 AND S2:S3
S14         8   RD  (unique items)
S15         7   S14 NOT PD>2001
S16      1661   (SERVER? OR WEB()SERVER)(5N)S10
S17         0   S16 AND S3
S18         7   S3 AND S10
S19         4   RD  (unique items)
S20         0   S12 AND S3
S21       764   S12 OR S3
S22         9   S21 AND S7
S23        48   S21 AND S6
S24        50   S22:S23
S25        29   S24 AND S1(5N)S4:S5
S26         1   S3 AND S1(5N)S4:S5
S27        18   RD S25  (unique items)
S28        13   S27 NOT PD>2001
File   9:Business & Industry(R) Jul/1994-2006/Mar 09
         (c) 2006  The Gale Group
File  13:BAMP 2006/Feb W4
         (c) 2006  The Gale Group
File  15:ABI/Inform(R) 1971-2006/Mar 09
         (c) 2006 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2006/Mar 10
         (c) 2006 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2006/Mar 09
         (c) 2006 The Gale group
File  75:TGG Management Contents(R) 86-2006/Feb W4
         (c) 2006 The Gale Group
File  88:Gale Group Business A.R.T.S. 1976-2006/Mar 03
         (c) 2006 The Gale Group
```

File 98:General Sci Abs 1984-2004/Dec
(c) 2005 The HW Wilson Co.
File 141:Readers Guide 1983-2004/Dec
(c) 2005 The HW Wilson Co
File 148:Gale Group Trade & Industry DB 1976-2006/Mar 08
(c)2006 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2006/Mar 08
(c) 2006 The Gale Group
File 369:New Scientist 1994-2006/Aug W4
(c) 2006 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
(c) 1999 AAAS
File 484:Periodical Abs Plustext 1986-2006/Mar W1
(c) 2006 ProQuest
File 553:Wilson Bus. Abs. 1982-2005/Jan
(c) 2006 The HW Wilson Co
File 610:Business Wire 1999-2006/Mar 10
(c) 2006 Business Wire.
File 613:PR Newswire 1999-2006/Mar 10
(c) 2006 PR Newswire Association Inc
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Mar 09
(c) 2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Mar 10
(c) 2006 McGraw-Hill Co. Inc
File 634:San Jose Mercury Jun 1985-2006/Mar 09
(c) 2006 San Jose Mercury News
File 635:Business Dateline(R) 1985-2006/Mar 09
(c) 2006 ProQuest Info&Learning
File 636:Gale Group Newsletter DB(TM) 1987-2006/Mar 09
(c) 2006 The Gale Group
File 647:CMP Computer Fulltext 1988-2006/Mar W4
(c) 2006 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Mar W1
(c) 2006 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2006/Mar 09
(c) 2006 Dialog
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc

13/3,K/1 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

02038749 Supplier Number: 25552255 (USE FORMAT 7 OR 9 FOR FULLTEXT)
DVD **body sues to halt decryption code's spread**
(DVD **Copy Control Association Inc files suit in effort to stop proliferation of DeCSS software program on the Web; program can copy encrypted video portion of a** DVD disk)
Electronic Engineering Times, p 6
January 03, 2000
DOCUMENT TYPE: Journal ISSN: 0192-1541 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 770

(USE FORMAT 7 OR 9 FOR FULLTEXT)
DVD **body sues to halt decryption code's spread**
(DVD **Copy Control Association Inc files suit in effort to stop proliferation of DeCSS software program on the Web; program can copy encrypted video portion of a** DVD disk)

ABSTRACT:
The **DVD** Copy Control Association Inc (Morgan Hill, CA), the licensing agency responsible for **DVD** security, has filed suit at the Santa Clara County office of the California Superior Court...
...software program from the Internet. The program can copy the encrypted video portion of a **DVD** **disk** . The agency claims the future of the **DVD** format is at stake. The agency also wants a restraining order to stop linking to...

...software claim it was developed as part of an effort to build a Linux-compatible **DVD** reader, which must carry a file containing one of the 400 "master keys" included on every **DVD** **disk** . The development of this reader and the software, as well as the lawsuit, are further...

TEXT:
By: Craig Matsumoto

SAN JOSE, CALIF. - The licensing agency responsible for **DVD** security has gone to court to stem the spread of hacked code that can thwart **DVD** encryption.

At stake, the plaintiffs assert, is the future of the **DVD** format itself. But supporters of the **DVD** hack disagree. They point out that the **DVD** encryption was cracked not for piracy but as part of a project to develop a Linux-based **DVD** player, something the **DVD** industry itself has yet to tackle. Meanwhile, some are calling for increased proliferation of the **DVD** hack as a way to protest the lawsuit.

...

...filed Dec. 27 at the Santa Clara County office of the California Superior Court, the **DVD** Copy Control Association Inc. (Morgan Hill, Calif., www.dvdcca.org) sought a restraining order forcing...

...for DeCSS, a small software program that can copy the encrypted video portion of a **DVD** **disk** .

In addition, the **DVD** group wants the restraining order to forbid linking to Web sites that contain any of...

...to DeCSS code.

The complaint, which activists have posted on the Web at cryptome.org/ **dvd** -v-500.htm, lists 72 offending Web sites. Twenty-one defendants are mentioned by name, and five of those reside outside the United States.

The **DVD** CCA has been sending cease-and-desist letters to some Web page owners since the...

...first to post DeCSS code to the Web. Johansen is not listed as a defendant.
DVD CCA representatives were unavailable for comment. In a prepared statement, they said they have worked...

...lawsuit was filed.

According to the complaint, "Without the motion picture companies' copyrighted content for **DVD** video, there would be no viable market for **computer** **DVD** **drives** and **DVD** players, as well as the related computer chips and software necessary to run these devices, and thus there would be no **DVD** video industry."

Indeed, some manufacturers have put off releasing **DVD** audio players, citing the hole in security (EE Times Dec. 6, 1999, page 1). Some manufacturers estimate it will take six months to revamp the security scheme.

In addition, the **DVD** CCA may have filed the suit in self-defense. Incorporated in Dela-ware, the **DVD** CCA describes itself as a not-for-profit trade association formed to handle licensing administration for the **DVD** industry. Just as DeCSS allegedly threatens the **DVD** manufacturers, it also threatens "the very existence of **DVD** CCA" and could lead to the demise of the association, according to the complaint. The...

...useful. Some call for widespread proliferation of DeCSS to toss a monkey wrench at the **DVD** CCA; one poster likened the strategy to the "whack-a-mole" carnival game.

Meanwhile, some...

...code is available.

Linux project

DeCSS started with an effort to build a Linux-compatible **DVD** reader. A **DVD** reader must carry a file containing one of 400 "master keys" included on every **DVD** **disk** . These **keys** identify **authorized** **DVD** players.

While **reverse** -engineering the **DVD** specification, programmers found that Xing Technologies Corp. had not encrypted its **DVD** master key. That helped open up CSS and led to the creation of DeCSS.

The **DVD** body worries that some of CSS's inner workings have been disclosed. CSS must be kept secret to prevent **DVD** piracy, the complaint charges.

The Electronic Frontier Foundation has provided a lawyer to represent the ...

...of the California Superior Courthouse in San Jose on Dec. 29, as a hearing considered **DVD** CCA's bid for a temporary restraining order.

Java programmer Andrew McLaughlin, a defendant, insists DeCSS aims to bring **DVD** to Linux and poses no new threat of piracy for **DVD** titles. "It was the opportunity to distribute software that would help people watch DVDs on ...

COMPANY NAMES: **DVD** COPY CONTROL ASSOCIATION INC

13/3,K/2 (Item 1 from file: 13)
DIALOG(R)File 13:BAMP

00685573 Supplier Number: 25611868 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Cracking DVD
(To prevent illegal copying, the movie industry chose to store films in a special format known as digital video **disc**)
Article Author(s): Wang, Wallace
Boardwatch Magazine, v XIV, n 3, p 134,136
March 2000
DOCUMENT TYPE: Journal ISSN: 1054-2760 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1142

(USE FORMAT 7 OR 9 FOR FULLTEXT)
Cracking DVD
...(the movie industry chose to store films in a special format known as digital video **disc**)

ABSTRACT:
Presented is a discussion on digital video **discs** (**DVD**). Unlike ordinary audio compact- **discs** (CDs), DVDs make use of a special encryption called the Content Scrambling System (CSS) to prevent illegal copying. **DVD** encryption varies according to one of six regions arbitrarily dividing the world. Such arbitrary division of the world into regions help limit the spread of any illegal copying. A **DVD** **disc** can only be played on **DVD** players designed for a specific region. Some groups found flaws in the CSS employed by...

...flaw in CSS encryption. DoD uncovered the encryption flaw and created its own program called **DVD** Speed Ripper for copying **DVD** **discs** . Initially, the program failed to copy all types of **DVD** **discs** . Once the DoD group fixed the problem, the MoRE group incorporated the changes in its ...

...called DECSS. The DECSS program is a small 60KB program that can copy an encrypted **DVD** file to a hard **disk** without using the protective layer of encryption. Article includes a discussion on the lawsuits slapped by the **DVD** Copy Control Association on Web sites offering the DECSS program.
...

TEXT:
...has haunted the entertainment industry since the days when people started copying albums using ordinary **tape** cassettes. The software industry battled the next wave of pirates by adding clumsy copy-protection schemes to keep people from copying floppy **disks** containing games or business programs.

Software publishers temporarily foiled software pirates by switching from easily-copied floppy **disks** to compact **discs** , but it was only a matter of time before re-writable **CD - ROM** drives became commonplace on virtually every new computer, giving everyone the technology to copy entire CDs on their home computers as easily as copying a floppy **disk** .

Understandably, the movie industry hesitated about putting feature films on compact **discs** . If software pirates could copy movies on **CD** as easily as they copied programs such as Microsoft Office 2000 or Windows NT, the movie industry would stand to lose millions in royalties alone.

THE BIRTH OF **DVD**

To prevent illegal copying, the movie industry decided to store films in a special format known as **DVD** (which stands for Digital Versatile **Disc** or Digital Video **Disc**). Unlike ordinary audio CDs, **DVD** **discs** use special encryption to prevent illegal copying, called a Content Scrambling System (CSS). To play a CSS-encoded movie, your **DVD** player needs a 5-byte (40-bit) decryption key.

For additional protection, **DVD** encryption varies according to one of six regions arbitrarily dividing the world. The regions are...

...the world into regions helps limit the spread of any illegal copying. To play a **DVD** **disc** , you need a **DVD** player, which can be a chunk of hardware like an ordinary audio **CD** player or a program that runs on a **computer** . **DVD** players (**hardware** or software) can only play **DVD** **discs** designed for a specific region.

For example, a **DVD** **disc** from China (Region 6) would not work in a **DVD** player sold in North America (Region 1). So even if hackers in Asia found a way to illegally copy **DVD** **discs** from Hong Kong, they could only distribute their pirated **DVD** copies within a limited region. While not eliminating potential piracy, it does limit the spread of illegal **DVD** copying. (For more information about the basics of **DVD** , visit www. **dvd** .com.)

CRACKING CSS

When copy-protected floppy **disks** arrived, computer crackers pored over the details until they found a way to duplicate copy-protected **disks** . So when **DVD** **discs** arrived with encryption, crackers all over the world examined it carefully, searching for flaws.

Contrary...

...to a paper jointly written and posted by both groups at http://02.uio.no/ **dvd** /codefree/decss.html, DoD discovered the encryption flaw first and developed a program called **DVD** Speed Ripper, for copying **DVD** **discs** . However, the **DVD** Speed Ripper program initially failed to copy all types of **DVD** **discs** . Once the DoD group fixed this problem, the MoRE group incorporated these changes in its own program called DeCSS.

In addition, the two hacker groups didn't actually crack the **DVD** encryption. Instead, they exploited a fatal mistake. To protect the encryption of **DVD** **discs** , all companies making **DVD** players and software must encrypt their **DVD** decryption **keys** to prevent **reverse** -engineering. However the XingDVD player, made by Xing Technologies, a subsidiary of RealNetworks, failed to...

...due to human error rather than any flaw in its encryption algorithm. As a result, **DVD** encryption is pretty much useless in preventing illegal copying of **DVD** **discs** .

HOW THE DECSS PROGRAM WORKS

The DeCSS program is a small 60 KB program that can copy an encrypted **DVD** file (which has a .VOB extension) to a hard **disk** , minus the protective layer of encryption. Once copied to a hard **disk** , you can freely copy and distribute the unencrypted movie over the Internet. When rewritable **DVD** drives appear, you'll be able to copy **DVD** **discs** as easily as copying an ordinary floppy **disk** .

photo omitted

In the age of massive hard **disks** and faster Internet access courtesy of DSL and cable modems, transferring an entire movie file...

...9.4 gigabytes) may be cumbersome, but not impossible.

Since Internet access speeds and hard **disk** space are always getting faster, cheaper and larger, it's only a matter of time before **DVD** copying will become as common as **tape** recording albums off your stereo. (For more information about DeCSS, visit The Ultimate DeCSS Resource Site at www.pzcommunications.com/decss/main.htm)

THE LEGAL AFTERMATH

With **DVD** encryption defeated, the entertainment industry turned to a long-cherished defensive tactic -- lawsuits. The **DVD** Copy Control Association (CCA) diligently tracks any Web sites offering the DeCSS program and threatens...

...s site at www.2600.com.)

photo omitted

Unless manufacturers decide to scrap the current **DVD** format and develop a newer, more secure format, **DVD** copying will be available to anyone. Even if the industry quickly moves to a different...

...publicize any fatal flaw.

Copyright enforcement has always been difficult, and the latest debacle over **DVD** merely highlights this fact. No matter what you protect, there will always be a way...

PRODUCT NAMES: Motion picture and video **tape** production (781200)

28/3,K/10 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01385605 SUPPLIER NUMBER: 09683355 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Providing software protection capability or a CD - ROM **drive. (technical)**
Nielsen, Kenneth R.
Hewlett-Packard Journal, v41, n6, p49(5)
Dec, 1990
DOCUMENT TYPE: technical ISSN: 0018-1153 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 4223 LINE COUNT: 00313

Providing software protection capability or a CD - ROM **drive. (technical)**

ABSTRACT: A **CD - ROM** can hold many large software packages on one **disk** , which can provide significant cost savings over **tape** distribution but poses a security problem. Load-time security, which permits customers to load a package from the **disk** only with proper authority, is the method used for the Hewlett-Packard Model 600/A...

...run-time security. Another method used on the 600/A is scrambling data on the **disk** to prevent reading a protected **disk** with another **CD - ROM** reader. A security toolbox can be used by the customer. The tools include the capability to lock and unlock discrete portions of the **disk** selectively, unscramble or decode secured data, and the ability to give the host a unique...
... security, which prevents loading a package without the proper authority, and scrambling data on the **disk** to prevent reading a protected **disk** with another **CD - ROM** reader.

AN EFFECTIVE USE of **CD** -ROMs is for the distribution of very large quantities of software and literature. Before **CD - ROM** technology, software updates were distributed on **tape** . This method required the creation of multiple customized **tapes** for each customer. The **tapes** contained only the software that the customer had purchased. The security solution with this method was simple-customers only received **tapes** for the packages they had purchased.

With **CD - ROM** as the distribution medium, many large software packages can fit on one **disk** . This capability provides a significant cost savings over the **tape** distribution method. The problem with using **CD** -ROMs for distribution is how to give customers many software packages on one **disk** yet restrict them from using software that they did not purchase. This article discusses some aspects of the HP Series 6100 Model 600/A **CD - ROM** drive security scheme.

Implementation Considerations

Two security schemes were considered for the HP Model 600...

...security.

Load-time security does not allow the customer to load a package from the **disk** without the proper authority. This is the method we decided to use for the Model...

...satisfies both of the constraints mentioned above. The authority for accessing packages on an HP **CD - ROM** is a unique password that is shipped to the customer with each **disk** . This password enables customers to identify themselves uniquely to the Model 600/A **CD - ROM** drive.

Security Toolbox

There are many opinions on and methods of implementing software security features...

...provided in the toolbox include:

* The capability to lock and unlock discrete portions of the **disk** selectively
* The ability to unscramble or decode secured data
* The ability to provide the host...

...The security scheme implemented may be defined in the security information that goes on the **disk** when it is mastered. This information may also define which host-to- **disk** commands (Command Set 80 commands) the Model 600/A will accept from the host.

The security information for a **disk** is located in the **disk** 's system area. When a **disk** is mounted in the drive, based on the information in the system area, the Model...

...redefines the default values of certain parameters. The default values are used when a new **disk** is loaded and after a Security Clear command is received from the host.

Region Access Map

The capability to lock and unlock regions of the **disk** selectively is provided using a structure called a region access map, which is located in the system area of the **disk** . The region access map logically divides the **disk** into regions. Each region has one or more logical sectors and each region is assigned...

...lock or unlock. A default group access map exists in the system area of the **disk** . The group access map is a string of bits with the value of each bit...

...and a verification password must be sent from the host to the Model 600/A **disk** controller. The **disk** controller will do some manipulation on the group access map, the publication identifier from the **disk** , and the internal identifier of the **disk** controller. The result of the manipulation is compared with the verification password received from the host. If the comparison proves that the group access map, the **disk** , and the **disk** controller all belong together, the customer's group access map is accepted as defining the locked and unlocked groups on the **disk** . If not, the HP Model 600/A **disk** controller will use the default group access map located in the system area of the **disk** . Fig. 2 summarizes this process.

To keep anyone from setting up a computer and sending files that might exist on a software distribution **disk** . The operating system is contained in logical sectors 0 through 500, the COBOL compiler in...

...both use drivers located in sectors 701 through 750. The region access map contains the **disk** addresses of each file. All the operating system files are assigned to group 0, the...

...to locked (see Fig. 3c). Because there may be hundreds of software packages on a **disk** , it would be easier if the customer did not have to type in the group...

...that the customer can unlock only purchased software.

When the customer tries to access the **disk** , a host program will ask the customer for the password that came with the **disk** . The program will send the group access map and the password to the Model 600/A **disk** controller, and after performing the comparison process described earlier, the controller will unlock the correct portions of the **disk** . Once the **disk** is unlocked, it can be read using any standard CS-80 driver.

if the host does try to access a locked portion of the **disk** , the

Model 600/A will normally respond with a NO DATA FOUND fault. However, there...

...to find out if an attempt was made to access a locked region of the **disk** and that invalid data was transmitted.

Unscrambling Data

The lockable **disk** is only secure if it is mounted in the Model 600/A **CD - ROM** drive. To prevent reading the **disk** from another **CD - ROM** reader, the data on a distribution **disk** is scrambled. The Model 600/A can unscramble a **disk** that has its data scrambled. This option should protect the packages from being loaded via...

...Model 600/A is an 8-byte value that can be located either on the **disk** or sent from the host. If the **key** is on the **disk** and scrambled, it is decoded using a predefined algorithm. If the key is sent from...

...be decoded using an algorithm that is unique to each customer's Model 600/A **CD - ROM** drive. This scheme allows each of several customers to have a unique key even if...

...for unscrambling data can be used in different ways. One method unscrambles either the whole **disk** or selected portions of the **disk** when data is read from the **disk** and sent to the host. Another method involves the host's using the Model 600...

...a package are scrambled. If the key used to unscramble the data is on the **disk** , the default method is to unscramble all data as it is read from the **disk** (see Fig. 4 **switch** position 2). If the **key** is sent from the host, the default method is to read the data and leave...

...600/A as an unscrambling box the host reads a complete scrambled file from the **disk** and then **sends** a customer-unique deciphering **key** to the **CD - ROM** drive. The host's unscrambling algorithm is a write, unscramble, and read sequence. First the...

...the host commands the controller to unscramble the data in the buffer using the deciphering **key** **passed** down earlier (see Fig. 4 switch position 1). Finally, the host uses the CS-80...Command Protocol

The HP-IB Command Set 80 protocol is used for communication between the **CD - ROM** reader and the HP 3000 MPE VE operating system. To simplify integration and for initial system startup the Model 600/A looks like a writeprotected HP 7935A 300-megabyte **disk** to the HP 3000 MPE VE operating system.

Making the Model 600/A look like...

...was simple. The biggest problem was trying to support the Release command, which frees a **disk** to be removed from the drive. Without a button on the front panel of the Model 600/A, the customer cannot request that the **disk** be released. On the HP 7935A, if the customer wants to remove a **disk** , the front-panel release button is pressed and the HP 7935A executes a release sequence that essentially asks the host if it can release the **disk** and go off-line, allowing the user to remove the **disk** and replace it with another **disk** . The HP 3000 system recognizes this sequence and knows that a **disk** has been removed and possibly replaced.

On the Model 600/A, if the door is unlocked, the user can remove a **disk** caddy at any time. It would be meaningless to make a Release request to the host because if the host denied the request, the host would think that the same **disk** was still loaded. The solution to this problem is that when a **disk** is removed a report is sent to the host that a new **disk** of zero length has just been loaded.

The constraint of trying to look like a...
...protected HP 7935A meant that commands specific to the security or audio features of the **CD - ROM** had to be added under the CS-80 initiate Utility command. Service
Servicing the Model...

...service engineer must have a means of programming these numbers in the field when a **CD - ROM** drive's controller board is replaced. The alternative to this would be to return the...

...the repair controller board serial number back to REPAIRBD. The process requires that a special **disk** be mounted into the drive before a second special service command (Service 11) is executed. The combination of the special **disk** and the bytes sent with the Service II command will reprogram the serial number REPAIRBD...

...Service II command is attempted and proves to be an invalid command because the wrong **disk** is being used or the wrong bytes are sent to the model 600/A, the...

...factory for reprogramming.
Utility Commands
The utility commands are CS-80 commands developed to support **CD - ROM** capabilities, security toolbox functions, and status information relevant to the Model 600/A security scheme...

...are not in the formal CS-80 definition but fit into the CS-80 protocol. **CD - ROM** Commands. The following CS-80 commands are designed to support the Model 600/A and the features of **CD** -ROMs.
* Door Lock. Lock the drive's media door to prevent unwanted removal of the **disk** .
* Door Unlock. Unlock the drive's media door to allow removal of **disk** .
* Play Audio (length of play) (address of audio portion of the **disk** where to start playing). Play an audio portion of the **CD - ROM** . This command will return to the report phase when the audio is finished.
* Play Audio With Return Address (length of play) (address of audio portion of the **disk** where to start playing). Play an audio portion of the **CD - ROM** . This command will have multiple execution phases. At the end of each execution phase the...

...of that track and the control and address field from the Q channel of the **CD - ROM** .
* Set Logical Sector Length (sector length). This command will modify the logical length of a...
...will be either 256 bytes or the length defined in the system area of the **disk** . The typical frame of an industry-standard **CD - ROM** written with computer data contains 16 bytes of header, 2048 bytes of data, and 288 will return data from the data field. If the **disk** has data for which data integrity is not important (e.g., video data), the ECC...

...minus the header field). The 2352-byte length will return the full sector. If the **CD - ROM** is a secured **disk** , this command is disallowed.
Security Toolbox Commands. These are the CS-80 commands that implement...

...the data fill capability. If data fill is enabled when a locked region of the **disk** is encountered, the fill word will finish the rest of the current transaction and the...

...data fill is disabled, the current transaction will abort when a locked region of the **disk** is encountered and the NO DATA FOUND fault is set.

* Unscramble Buffer (length of data...

...1).

* Unscrambled Read on/off). This command will either send the data stream from the **disk** through the unscrambling algorithm (on) or not (off) before sending the data to the host...

...cause the contents of the controller's data buffer to be returned to the host.

* **Receive** Data Unscrambling **Key** (**key**). This command will cause the **key** **received** to be manipulated by the Model 600/A's unique identifier algorithm and then be used as the unscrambling **key** for future unscrambling.

* **Receive** Group Access Map password)(group access map). This command will cause the received group access map to be accessed if the password, the group map, and the currently loaded **CD** - **ROM** 's identifier all belong together.

* Return Drive Security Number. This command will cause the Model...

...4).

Security Status Commands. The following commands were added to retrieve status information about the **CD** - **ROM** and to make the security toolbox easier to use.

* Report Security Quick Status. This command will return one byte that indicates powerfail, **disk** change, and/or a security fault. This status is cleared either by a Security Clear...

...Request Security Status. This command will return a string of bits indicating the type of **disk** currently loaded, the security features that are present in the system area of the **disk** , and the security faults that have occurred. This status is cleared either by the Security...

...and the Security Clear command is that the CS-80 Clear command will set the **CD** - **ROM** reader and all internal state machines back to power-on conditions. The Security Clear command will set the security features back to either power-on or new **disk** loaded conditions. Using the Security Clear and the CS-80 Clear commands independently will help...

...commands.

Conclusion

The tools designed into the HP Series 6100 Model 600/A HP-IB **CD** - **ROM** drive should be adequate for almost any user who wants to distribute software or data on **CD** - **ROM** **disks** . The **disk** publisher can tailor the security level to range from no security at all to a...

...to the host CS-80 driver, the commands are available to do so. If the **disk** distributor wants to change the unique customer password verification number, there are hooks built into...

...the distributor and the customer.

Acknowledgments

The HP Series 6100 Model 600/A HP-IB **CD** - **ROM** drive project was a joint effort between HP's Greeley Storage Division (GSD) in Greeley...

...CAPTIONS: regions, and logical sectors. (chart); Process for determining the locked and unlocked areas of a **disk** . (chart); Steering unscrambled data in and around the Model 600/A's unscrambler. (chart)

...DESCRIPTORS: **CD** - **ROM**

TRADE NAMES: HP 6100 600/A (**CD** - **ROM** drive...